INFORMATION SECURITY MANAGEMENT AT THE U.S. DEPARTMENT OF VETERANS AFFAIRS—CURRENT EFFECTIVENESS AND THE NEED FOR CULTURAL CHANGE

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON VETERANS' AFFAIRS
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

FEBRUARY 28, 2007

Serial No. 110–5

Printed for the use of the Committee on Veterans' Affairs

U.S. GOVERNMENT PRINTING OFFICE
34–307 WASHINGTON : 2007

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

Pursuant to clause 2(e)(4) of Rule XI of the Rules of the House, public hearing records of the Committee on Veterans' Affairs are also published in electronic form. **The printed hearing record remains the official version.** Because electronic submissions are used to prepare both printed and electronic versions of the hearing record, the process of converting between various electronic formats may introduce unintentional errors or omissions. Such occurrences are inherent in the current publication process and should diminish as the process is further refined.

CONTENTS

FEBRUARY 28, 2007

INFORMATION SECURITY MANAGEMENT AT THE U.S. DEPARTMENT OF VETERANS AFFAIRS—CURRENT EFFECTIVENESS AND THE NEED FOR CULTURAL CHANGE

WEDNESDAY, FEBRUARY 28, 2007

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON VETERANS' AFFAIRS,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:36 p.m., in Room 334, Cannon House Office Building, Hon. Harry E. Mitchell [Chairman of the Subcommittee] presiding.

Present: Representatives Mitchell, Walz, Rodriguez, Davis, Brown-Waite, Stearns.

OPENING STATEMENT OF CHAIRMAN MITCHELL

Mr. MITCHELL. The Subcommittee on Oversight and Investigations hearing of February 28, 2007, will begin.

Let me just say right off that Congressman Zach Space is absent because of a family emergency. Otherwise, he would be here.

I have accelerated our Subcommittee's review of the VA information security management for several reasons.

I thank all three panels of witnesses and our Subcommittee Members for their cooperation despite the somewhat short notice we were able to provide. It is my belief that when the subject matter justifies some sort of review that such a review should be thorough, balanced, and timely.

This topic was on the Subcommittee agenda for later this year, but it is a recurring and nonpartisan topic for the Veterans' Affairs Committee. The events regarding a data loss at Birmingham and other circumstances have led me to advance this hearing on our Subcommittee docket.

In this hearing, I wish to determine the current status of information security management at the VA. Admittedly the Birmingham incident holds powerful sway over the landscape. If the Birmingham incident stood alone against the backdrop of a sound information security management program, perhaps we could address a one-time-only incident with more patience.

However, the record reflects a host of material weaknesses identified in consolidated financial statements, audits and the "Federal Information Security Management Act," FISMA, their audits over the recent years.

The Inspector General's Office and the Government Accountability Office have both reviewed VA and found deficiencies in the information security management program over the last 8 years. VA has been slow to correct these deficiencies.

For example, the VA IG made 16 recommendations with regard to information security management in 2004. All 16 remained open in 2006.

During our full Committee review of the May 3, 2006, data loss, we discovered a general attitude regarding information security at VA that our current Committee Chairman Bob Filner once referred to as a culture of indifference.

Today I wish to address this issue of culture and the need for cultural change with regard to information security at the VA.

Last year, the Committee reviewed cultural problems at several levels at VA. We looked at the very top levels of the VA leadership and were critical. We looked at the program leadership levels and were critical. We looked at the promulgation of information security policy in VA and were critical of the various methods employed by some program leaders and advisors to gut those policies to avoid accountability of the weakened information security practices. We were critical of the lack of checks and balances in the information security management system at VA.

Guidance was being followed, but did oversight occur? We were critical of delay by VA in providing congressional notice of the May 2006 incidents. We were critical of the slow escalation and notice of the magnitude of that problem.

VA mailed notices to millions of veterans addressing the data compromise and made a public commitment to become the "gold standard" in information protection within the Federal Government. Eight months after the initial data loss, VA reports another loss of significant magnitude associated with Birmingham VA Research Program.

That a weakness existed in this area surprised no one. That it happened at all serves to precipitate this type of congressional oversight hearing. While the actual loss of the external hard drive and the limited electronic protections on that missing equipment should be considered the 800 pound gorilla in this room, there were some silver linings with the Birmingham story as we now know.

For example, the loss was reported in VA and quickly relayed to the appropriate people. Mr. Howard notified congressional oversight staff and Secretary Nicholson called the Chairmen and Ranking Members of the VA Committees. The Office of Inspector General was quickly involved and opened an investigation.

In similar examples from May 2006, VA took days or weeks to accomplish those tasks. In the Birmingham incident of January 9, 2007, VA took hours or days to accomplish the same task.

Staff was notified within 1 day and calls from the Secretary followed a few days afterward. The investigative trail was reasonably fresh for the IG to follow.

What of VA culture with regard to this issue? The IG made five recommendations to the Secretary in the review of issues related to the loss of VA information involving the identity of millions of veterans on July 11, 2006. As of today, all five of those recommendations remain open. Why?

After the 2006 series of hearings, VA issued a series of tough-sounding declarations, but problems still remain and another major incident has happened.

After the Birmingham incident, the Secretary issued some tough guidance, but what impact will it have? Will history repeat itself? How deep are the cultural barriers?

I believe that it is important to review all aspects of this issue. We need to hear from VA leadership and in that regard, we are pleased that Deputy Secretary Mansfield has agreed to testify. He, Secretary Nicholson, the Under Secretaries are key to setting policy. They represent the Department in this matter.

But we also need to look at the problem through the eyes of the remaining 200,000 plus people in the VA. Do leadership actions throughout the management hierarchy match policy guidelines everywhere in the VA? Do the rules say no, but the culture beckons, ah, go ahead, make an extra copy of that data and your own life will be easier? Take a shortcut. No one will follow up.

If we change the culture of VA, we can begin to fix the problem. But people have different cultural perspectives. Those of the VA leaders on panel one may differ from those of the researchers in the field. Leadership's policy guidance may now be spot on, but the question is how the policy is received at the user end.

For that reason, this Subcommittee requires testimony across the spectrum of people who in any way handle sensitive information about our veterans. Let us approach this with open minds, consider other perspectives, and be able to put this problem to rest for a long time.

Before I recognize the Ranking Republican Member for her remarks, I ask unanimous consent that Congressman Artur Davis from Alabama and Congressman Spencer Bachus be invited to sit at the dais for the Subcommittee hearing today. Without objection. Thank you.

I now recognize Ms. Brown-Waite for her opening remarks.

[The statement of Harry E. Mitchell appears on pg. 54.]

OPENING STATEMENT OF HON. GINNY BROWN–WAITE

Ms. BROWN-WAITE. I thank the Chairman very much for giving me this opportunity and also for the expedited manner in which this hearing was held.

As the Chairman has indicated, it is more about information security management at the Department of Veterans Affairs and in particular the current effectiveness of information security at the Department and the need for cultural change.

Since the data breach in May 2006, which was the second largest in the nation and actually the largest in the Federal Government, we have seen VA's centralization of the VA's information management, including information security.

I appreciate the Secretary's desire to make the VA the "gold standard" for information technology and information security management in the Federal Government. From what we have seen, however, adherence to the "Federal Information Security Management Act" or FISMA has not been adequately addressed government-wide as Congress intended when writing the law.

This is why our Committee worked so hard last Congress to pass measures such as H.R. 5835 and the final version which was S. 3421 which eventually became Public Law 109–461.

We have tried to give the Department, and in particular the Secretary, all the tools that he needs to mandate change within the entire Department to make certain that such security breaches are few, if any.

I served on this Committee now, this is my fifth year, and recently have been selected as the Ranking Member of this Subcommittee. Over the years, however, I have seen a blatant lack of resolve within the underlying culture at the Department and particularly at the facility level to change the way senior management view IT security.

We know it is very difficult to embrace change, but this is what we need to address in this hearing. I was involved at one point in my life in installing a new financial management system for my employer, and I can just tell you that the employees were kicking and screaming because change does not come easily. They were used to their little silos and they really did not adapt very well to any kind of IT change.

I realize that this is a problem that is out there in the VA, but it is not one that with very strong leadership we cannot overcome. We have got to protect our veterans and provide them with the services that we need. We need to remove that cultural bias against change.

I appreciate the witnesses who have come to this hearing, particularly those who have traveled great distances to be here. And I look forward to hearing your testimony.

I thank the Chairman, and I yield back the balance of my time.

[The statement of Ginny Brown-Waite appears on pg. 55.]

Mr. MITCHELL. Thank you.

Mr. Walz.

OPENING STATEMENT OF HON. TIMOTHY J. WALZ

Mr. WALZ. Thank you, Mr. Chairman. Just briefly, thank you for holding this important hearing.

As a veteran who has received the letter earlier on lost data, this is obviously one that is personal to me and it is also one that everybody in this room cares deeply about.

Mr. Mansfield, thanks so much for coming here. And I know that everyone in this room and at the table care as deeply as anybody about our veterans and making sure everything is done right.

So I hope that in this hearing, and in the spirit of the Chairman's words, that we are here to find solutions, that we know that the intent of every member of the VA is always to provide the best quality care, the best quality protection to our veterans. So I thank you for being here.

The one thing I would say, I guess for me, I am a cultural studies teacher, so this idea of culture and the things that we talk about, all those learned and shared values, beliefs, and ideas, I think is critical. Whether it is a safety issue or whether in this case it is data security, that I do believe culture plays a roll in it.

And we are here today to figure out what we can do if it is a resource issue or what we can do. And I truly appreciate your will-

ingness to come and all you do for veterans. And together we can get this thing worked out and get it going in the right direction. So thank you.

And I yield back my time, Mr. Chairman.

Mr. MITCHELL. Thank you.

Congressman Rodriguez.

OPENING STATEMENT OF HON. CIRO D. RODRIGUEZ

Mr. RODRIGUEZ. Thank you very much.

And I was just going over the report from the Inspector General and it is pretty startling information there in terms of the fact that there is still a great deal at risk.

I know the Attorney General in Texas just ruled that all county clerks that release Social Security numbers would be committing a felony. And so somehow we need to come to grips with that. And if I have to, I will make some of those comments at that time, but I am hoping that we can direct it in the right direction.

And I hope that the approach that is taken is that if you need some help, if you need some assistance, to come forward in order for us to correct this as quickly as possible.

Thank you.

Mr. MITCHELL. Thank you.

Mr. Bachus.

OPENING STATEMENT OF HON. SPENCER BACHUS

Mr. BACHUS. Thank you, Mr. Chairman.

I would say this to the panel. Since at least 1997, there have been reports about inadequacies at the VA, about the protection of information, veterans' information.

And in 2001, there were multiple recommendations made, 17 security recommendations made in the "Federal Information Security Management Act" for veterans to do. Yet, in May of 2006, when you had the security loss, Ms. Brown-Waite mentioned that none of those had been implemented at that time.

Now, since that time, you have given testimony to Congress that you fixed most of those problems. But what we had in Birmingham, it is my understanding, was just a laptop computer with information on it that was carried offsite. And to me, that is one of the most elementary types of things to prevent, simply by having a rule that they do not do that.

Now, you have also since last May, you required all veterans' employees to go to security seminars, as I understand it. So I would just be curious in my questions following up on whether that was done or not and whether this employee was prohibited from taking it offsite.

I know the IG's report says that the information that is available to all the employees is hard to understand and uses words like appropriate and other words which really will not limit them, you know, do not use the information inappropriately without clearly defining what may be appropriate and inappropriate.

But there are other issues. I know it was 21 days before it was announced that this breach had occurred. Another problem that I had with this as a Member of Congress, Congressman Davis and I represent the Birmingham area and a lot of this information was

shared with us, but we were told we could not share any of the information with anyone else, that it was critical to the investigation. And one occasion, after we were specifically told we could not share any of the information, it was critical to the investigation, within an hour, the Veterans Administration issued a press release with a lot of that information on it. So we wonder about that.

But I came here to listen, but I did come, and I have made this point to you gentlemen since this breach, that encrypting of information is a pretty elementary step. And I wonder why, you know, is there a rule that this information should be encrypted. I mean, a lot of this information was not encrypted which ought to, by 2007, ought to be standard operating procedure on any sensitive information.

And so I look forward to hearing from you. But it does appear that since 1997, at least 2001, everybody has known what problems were, that these were accidents waiting to happen, yet nothing. You know, if you did something as a practical matter, it did not work. So I would just be interested to know what you did.

Mr. MITCHELL. Thank you.

Mr. Davis.

OPENING STATEMENT OF HON. ARTUR DAVIS

Mr. DAVIS. Thank you, Mr. Chairman. I am glad to see that freshmen can become Subcommittee Chairs so quickly and I congratulate you on that. I must be on the wrong Committee.

Thank you for giving leave to my friend from Alabama and myself to come here. We are not regular Members of the Veterans' Affairs Committee, and I thank you for letting us participate because our City of Birmingham is affected.

I want us to get to the question section as soon as we can so I will be very limited in my comments. But I begin by saying this, Mr. Mansfield. I think all of us take it for granted that the leadership at the VA has good intentions, but good intentions are usually not enough to change a culture. Better laws help. Better regulations help.

And I received the correspondence that you sent to me in which I asked a number of questions about what the procedures are at the VA regarding encryption, what the procedures are at the VA regarding notification, and it is clear to me from looking at your answers that there are gaps there. And, frankly, that is where this institution comes into play.

Some of us have been advocates on this Committee for having stronger protections for civilians regarding potential losses of data, regarding data security issues in the private sector.

It seems self-evident to me that whatever the standard ought to be for individuals in the private sector, if anything, it ought to be stronger for our veterans. And I am disappointed. But if I understand the law and the regulations today, it is weaker. And understand some of us believe the consumer protections are not strong enough for civilians either.

Second point that I want to make, I have a very strong hunch, Mr. Mansfield, that the only reason we are in this room having this hearing, the only reason that the public knows about any of this

is simply by pure luck. And I do not mean to second guess, but I will make this point to you.

Your office called my office on the late afternoon of February 2nd, 2007, and you told us that you wanted us to have information about a data breach in Birmingham and you told us that a news organization was about to run with the story, so you wanted to give us a heads up.

I have a strong hunch, Mr. Mansfield, that but for you all believing this information was about to come in the public domain that you never would have released it.

Second of all, after the Office of Inspector General met with me at my request, we lodged a very strong demand of the VA that the VA go forward and release the additional information about the amount of names that had been compromised, about the fact that physician information had been compromised.

Frankly, I have a hunch that but for that demand, the additional information would not have been released.

So I will end with this point. Changes need to be made, in my opinion, in the way that your organization reacts to this kind of a problem.

I am going to ask you during my question time during the hearing how many data breaches are suspected by the VA since the incident of May 2006. We know about that incident. I am going to ask you during my Q and A session how much has been suspected in the year since. Are there other instances where there has been a loss of data? Are there other instances where there is a suspected loss of data?

So I thank you for being here, and I look forward to answers to your questions.

Mr. Chairman, thank you again.

Mr. MITCHELL. Thank you.

Mr. Stearns.

OPENING STATEMENT OF HON. CLIFF STEARNS

Mr. STEARNS. Thank you, Mr. Chairman, and thank you for holding this critical and timely hearing.

When you look at the GAO report, it says from 1998 to 2005, there were over 150 recommendations to the VA on implementing effective controls and developing a robust information security program.

And then if you just look at the VA's own Office of the Inspector General, they publish reports. They made 16 recommendations from the fiscal year 2004 and they remained unaddressed.

So we have here critical areas that are being highlighted by the GAO as well as the Office of Inspector General clearly saying the VA is vulnerable to denial of service attacks, disruption of mission-critical systems, and unauthorized access to sensitive data.

So all this has been documented. The Member before me talked about it is just by luck we have information about this. But I think we have known about this for some time, at least since January.

And so the question is with the GAO and the Office of Inspector General, why in the world are all these recommendations and all these suggestions not being implemented?

There has been a lot in the news recently regarding unauthorized access violations at the VA. Last March, there was an incident we had where 26 million veterans' information, personal information, personal, identifiable information was lost.

I congratulate the VA for finally getting the computer and getting the protection it needed, but, you know, it took a while to find it. And as I understand it, a lot of this information was not even encrypted.

And, however, now, in the recent breach that my colleagues have mentioned in Birmingham this January, the proper agencies were informed the very next day, an improvement that I would like to highlight, yet it is a mixed bag of praise and condemnation for we have yet another breach of information security.

This Birmingham hardware involved the personal medical records, Social Security numbers, personal information of veterans and many medical personnel in the VA system itself. And this information again was not even encrypted.

So it seems to me at this point, this information should be encrypted at the very least. There are clearly areas that the VA needs to improve. And I guess for the life of me, I do not understand. If you go back to 1998 and you have got 150 recommendations from the GAO, why are you folks not implementing them?

In Congress, we responded to the data breach of last March. We enacted the new law, the "Veterans Benefit Healthcare and Information Technology Act" of 2006. The primary purpose of this legislation was to strengthen IT practices at the VA. It also contained internal processing requirements regarding security management with a mandate, with a mandate for the VA to develop interim regulations for improving security within 180 days of the law's enactment.

So, Mr. Chairman, I think that the hearing is timely. I look forward to the witnesses, and I hope the strategy will be for improving security for our veterans in the very near future.

Mr. MITCHELL. Thank you.

We will now proceed to panel one. We are pleased to have Deputy Secretary Gordon Mansfield as the principal presenter for the panel.

This Committee has a long and professional working relationship with Mr. Mansfield in all his roles at VA, from his time serving as the Assistant Secretary for Congressional and Legislative Affairs to his present position as Deputy Secretary.

Mr. Mansfield is a highly decorated military combat veteran, having served two tours of duty in Vietnam. His military awards include the distinguished Service Cross, the Bronze Star, two Purple Hearts, and the Combat Infantry's Badge.

Mr. Secretary, would you please introduce your team.

Mr. MANSFIELD. Thank you, Mr. Chairman. If I may, before I start, a point of personal privilege. With your permission, I wanted to take a brief moment to comment on Len Sisteck's departure from the Committee.

May I have your permission, sir?

Mr. MITCHELL. Yes.

Mr. MANSFIELD. Len and I had a chance to talk the other day in my office, and he told me that he still had "the sense of service

to one's country" that we have seen up to this date. And I am pleased that he will continue as a public servant.

Many may say it, but Len has lived the concept of leaving political and ideological differences aside in order to serve veterans. He also got out and saw the VA operations in the field in a real hands-on way.

I mentioned he was in my office, on the tenth floor. I also want to make the point that Len has also been with us in our operations center down in lower basements, the bowels of the VA, so he has been with us from top to bottom.

I, for one, am glad that he will still be here on the Hill watching out for the interests of the Department and for veterans, just in a different capacity. Fairness and loyalty to the constituency are his, and I appreciated his service on this Committee. And I want to extend to him the congratulations and best wishes of the entire Department.

Len, thank you very much.

Mr. MITCHELL. Thank you, Len, very much.

STATEMENTS OF HON. GORDON H. MANSFIELD, DEPUTY SECRETARY, U.S. DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY MICHAEL J. KUSSMAN, M.D., ACTING UNDER SECRETARY FOR HEALTH, VETERANS HEALTH ADMINISTRATION, U.S. DEPARTMENT OF VETERANS AFFAIRS; HON. ROBERT HOWARD, ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY AND CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF VETERANS AFFAIRS; AND JAMES BAGIAN, M.D., CHIEF PATIENT SAFETY OFFICER, DIRECTOR, NATIONAL CENTER FOR PATIENT SAFETY, VETERANS HEALTH ADMINISTRATION, U.S. DEPARTMENT OF VETERANS AFFAIRS

STATEMENT OF HON. GORDON MANSFIELD

Mr. MANSFIELD. Mr. Chairman, if I may, I have a statement to submit for the record.

Mr. Chairman, I am here today with Mr. Howard, our Assistant Secretary for IT; the acting Under Secretary, Dr. Kussman; and Dr. Bagian.

I am here today to talk about the status of our IT security program and the reorganization of our Office of Information Technology.

We have done a lot of work and we have come a long way since last May's major incident occurred. And I have to admit that that was probably the wake-up call for the Department. But we still have an awfully long way to go.

We are well into the reorganization of the Office of Information and Technology to include an initial transfer of some 4,600 individual employees now under the control and direction of the CIO, Assistant Secretary Bob Howard.

That reorganization also includes ensuring that Mr. Howard has the full authority as delegated by the Secretary to deal with security issues throughout the Department. Mr. Howard also has the authority to oversee the total IT budget for the Department.

In the information security area, we have gone forward with preliminary revisions that have led us to issue a number of new direc-

tives to ensure that the workforce understands what their specific responsibilities are.

We have brought management pressure from the top to ensure that the required change in culture is instituted and that we are moving forward to achieve the goals set by the Secretary for the VA to be a gold standard for the Federal Government.

As I have stated, I think we have come a long way in both the reorganization and changes demanded by information security requirements to protect our veterans. I will be the first to acknowledge that we have not finished with either of these chores.

We are continuing the reorganization with more transfers of people taking place next month, with more budget, more program, and more people responsibilities under the control of the CIO.

The Security Operations Center or the SOC is now receiving daily reports of incidents, large and small, from across the Department which allow us to understand and educate the people that we are responsible for when they do the job wrong, and also it will allow management to get a better picture of the problem areas across the Department.

The Birmingham incident, while evidence of major lapses in judgment in operations, was handled in such a way that VA management was informed in a timely manner and the report moved quickly up the chain of command to the top.

We also started an investigation as did the Inspector General's Office in conjunction with the FBI. Notifications of the incident were made to the Hill in a timely manner. As well, updates on the information were provided as received.

I want to make a point here that as we get into these investigations and as the IG and the FBI move into it, we are requested that we keep this information on hold as they start into their investigation and start looking for areas of approach, and we try to follow the FBI's request and the IG's request in that area.

We have been notifying this Committee and other Committees of jurisdiction on the Hill on a weekly basis of the reports that do come in to us that are reported up the chain of command.

Another area of concern is sanctions applied to those who fail to conform to the requirements. The Secretary has said there are still too many VA employees at every level to include senior positions who either still do not comprehend the seriousness of this issue or who consciously disregard it.

This laxity is unacceptable and no longer will be tolerated. In appropriate cases and where justified, there must be serious consequences for failure to properly secure veterans' data. We owe our veterans no less. And that is a quote from the Secretary in a meeting of senior executives held here in Washington, D.C., on February 21, 2007.

We are involved in cultural change in a serious way. From the highest leadership on down, in meetings and communications and site visits, the Secretary and I have endeavored to communicate the need to protect data and how we can make that happen.

As the Secretary indicated, given the circumstances of each case, we need to go forward with further education and assistance with our employees to understand what the need is and what they have

to do or get involved in considering whether sanctions should be considered and applied as required.

In closing, let me say that I sincerely wish that I could promise you that no other incident will occur. I cannot do that now, but I can promise you that we are working hard throughout the Department to get the message to our 235,000 plus employees to do everything we can to get this problem under control.

We have succeeded in many areas. We still have a large job to finish the effort. We are committed to doing that.

Mr. Chairman, I am prepared to answer questions, and I would ask Mr. Howard, as I understand the sequence, to go forward with his comments.

Mr. MITCHELL. Correct.

[The statement of Gordon Mansfield appears on pg. 56.]

STATEMENT OF HON. ROBERT HOWARD

Mr. HOWARD. Thank you, sir.

And thank you, Mr. Chairman and Members of the Committee.

I would like to expand on Deputy Secretary Mansfield's comments regarding the changes underway in the area of information and technology.

There are two specific areas I would like to focus on. First is the extensive reorganization taking place and second is the over-arching program we have established to provide focus to all of our remediation efforts.

The IT realignment program to transition the VA's IT management system remains on track and is scheduled to be fully implemented by July 2008.

By April 1, 2007, software development employees and programs will be permanently reassigned to the CIO. This action follows the consolidation of operations and maintenance under the CIO which was finalized beginning this fiscal year.

We are implementing a process-based organizational structure rooted in best practice processes that are aimed at correcting IT deficiencies that resulted in a loss of standardization, compatibility, interoperability, and fiscal discipline.

There are 38 such processes that are being introduced with the assistance of IBM from a best practices standpoint. We have also developed a different organizational framework to provide focus in key areas.

The Office of Information and Technology is now comprised of five major organizational elements. These will all report to the CIO. We have a chart of this organization with us today in the event you would like to discuss this structure in more detail.

Each of the five major organizational elements is led by a Deputy Chief Information Officer. One Deputy Chief Information Officer, in fact, in the first column, is charged with directing the information protection and privacy programs in VA. This official is also responsible for risk assessment, risk mitigation, evaluation and assessment as it relates to information protection.

The DCIO for information protection and risk management has drafted the interim final regulation on credit monitoring and credit protection as required by the "Veterans Benefits Healthcare and Information Technology Act of 2006."

This regulation, which is now being reviewed throughout the Department, will address notification, data mining, fraud alerts, data breach analysis, credit monitoring, identity theft insurance, and credit protection services.

To achieve the gold standard as directed by the Secretary, we have implemented an over-arching program to assess information protection controls, to develop plans to strengthen the controls where necessary, to enforce the controls, and continuously monitor the information protection program.

This action plan we have developed includes development and issuance of policies and procedures, training and education, securing of devices, encryption of data, enhanced data security for VA's sensitive information, enhanced protections for shared data in interconnected systems, and incident management and monitoring.

A number of the specific requirements of the new law have already been introduced into our comprehensive action plan. I personally review progress on these actions on a weekly basis.

In closing, I believe we have made progress in improving IT operations in VA and we are working hard in partnership with the administrations and staff offices to improve our business practices to ensure the protection of sensitive information throughout the Department.

Mr. Chairman, that concludes my testimony. I would be pleased to answer any questions the Committee may have.

Mr. MITCHELL. Thank you.

Dr. Bagian.

[The statement of Robert Howard appears on pg. 58.]

STATEMENT OF DR. JAMES BAGIAN

Dr. BAGIAN. Thank you, Mr. Chairman, members of the Committee, for inviting me here today.

My comments will be confined more to cultural aspects, especially with respect to some of the observations of what we've done in the patient safety area, as I've talked to some of you in the past.

Let me just say at the outset, there has been some indication by some of the previous comments that people are wondering if people take the issue of IT security seriously. I can tell you unequivocally, they take it very seriously. There's nobody I see—and I am out in the field quite a bit—that is not fully aware that this is an important issue. There's no question about that. I'll come back to that, but, let me just assure you that's a fact.

The big issue is about culture and how we look at this. And I would say one of the big issues—and I'll talk about it from the frame of patient safety—because while our goal in patient safety is to prevent harm to the patient, and generally we think about that with regard to the medical care that we deliver, the fact is that if people suffer, for instance, the outcome of identity theft, for example, that harms them as well—as it harms our ability to provide care for them because that consumes fiscal resources and attention that could otherwise be focused to our primary mission, which in the VHA is delivering medical care. So we understand that.

In the safety area, patient safety area, when we started to do this some 8, 9 years ago, the culture certainly wasn't geared toward

patient safety, and we were starting this before anybody did it anywhere in medicine, quite frankly.

And we found that it was very important to be able to establish for them what our real goal was in terms that were understandable by them and how it met what they thought they needed to do. To create an expectation was relevant to them that they thought was real.

And then we had to go through an understanding when things did happen, it wasn't enough strictly just to have—and as Mr. Howard talked about, policies and training is important, but he talked about other things like encryption and other modalities. It's a multiplicity of these things.

It's not just telling people, "follow the rules," because if that is all it took to do anything, we'd write rules and go home. And we know it takes more than that. So, when problems occurred or we had close calls—as we have had IT close calls as well—it was to look and say what happened here, why did it happen, and what do we do to prevent it in the future?

And without understanding those underlying causes, it's really impossible to come up with sustainable solutions. So we really dwelled on that quite a bit, and I think you see some of that same thing in what's going on with the IT organization today.

The other thing is you have to take out the fear. One of the things that goes on with any organization, as was mentioned by Ms. Brown-Waite during her comments, is that change is hard for all organizations. And people have to feel that the change is in their interest, too, whatever that change is, and communicate to them what they believe it is. And I think we can do that, and we're trying to do it. But it doesn't happen overnight.

We then need to supply tools, and that's being done. You've heard about encryption. You've heard about other things that go in those areas. And then we have to do it in a way that changes their behavior, and when that behavior works and is not at cross purposes with their goal—and in VHA, the goal is delivering clinical care; that's the main goal—information security is embedded in that, but that's not the reason they come to work. A physician doesn't come to work to achieve IT security. It's a component thing they need to worry about, but their main goal is that they want to take care of the patient.

We have to understand how we make that real to them, that they understand that that's important not just because we say it is, because they believe it is. And I think that's trying to be done. So when that attitude changes, then you begin to change culture.

Now, one of the things that we found that was extremely important when we began was we thought everybody got it about patient safety. We did a cultural survey—the first one ever done—on attitude toward patient safety, and we found some very remarkable results which changed the way we ran the entire program and in fact, I would say we are singularly responsible for it being successful versus failing miserably.

We found that when we asked people, "Do you think patient safety is important?" Twenty-seven percent of all our people at the VHA system said "five" on a one-to-five scale. Patient safety is super important, most important it could be. Twenty-four percent

said "one"—absolutely irrelevant. We were shocked. How could that be?

But when we stopped and talked to them more—we've had focus groups come in to understand why that was—the reason they said "one,"—that is, unimportant, was because they said, "Well, I thought you meant was it important for me? It is not important for me, because I know I am safe. It is all those other people that aren't.

And the same thing can happen here if you don't understand what motivates them. It's not they do not want to do it. They think somebody else is doing it.

Until you really answer those questions to enable you to understand people's underlying assumptions, it's impossible to correct it effectively. So I think we need to look at that and look at the culture where it is and not just talk about it, but actually measure some of it to understand where the leverage points are. And I'm not sure we know all those things yet. But we're moving in that direction.

One of the things we worked with the IT system back in 2003 when the Blaster Worm—some of you may recall the Blaster Worm, a big problem—we went and worked with IT at that time. In fact, one of Mr. Howard's deputies—we talked last on the 21st, just last week, about how we worked with them with root cause analysis where we looked at these, what happened, why did it happen, what do we do about it—and he remarked that since that time we've never had a major denial of service attack, since we looked at this with a very systems-based approach. And they want to work with us more doing that, and we look forward to those kinds of things.

And we think this mode of collaboration across not just the IT world, but across all VA—DVA, NCA, VHA—working together to look at this and look at the real causes will get us there, and I think that's where the real hope lies, and it is not just having a knee jerk response to the bad events, which none of us want, but really take the time to understand why it isn't where we want it to be and fix it and really nail it.

[The statement of James Bagian appears on pg. 58.]

Mr. MITCHELL. Thank you all for your statements.

Clearly the VA is attempting a number of different avenues to address the problems associated with information security management at VA. We are aware of the poor track record the VA has in this area and note that implementing a program does not guarantee a successful outcome by itself.

Mr. Mansfield, I have a question. In 2006 and in earlier years, we saw information security policy guidance languish in various VA offices. The IG advises us in testimony that the VA still lacks a clear, concise policy in several key areas of information security. It has been 7 months since their report was issued.

Why do they say that and how do the views of the Department differ with the views of the IG?

Mr. MANSFIELD. Mr. Chairman, let me start by saying that we have proceeded and gone forward in a large number of areas and issued a large number of directives that deal with some of the issues that the IG is talking about.

The Secretary has issued directives and I have issued directives. I think what the IG is saying is that we have not been able to finalize this thing across the entire organization.

And I would make the point that in some of these areas, we are still learning about exactly what is happening out there, and we need to be able to find out what the issues are and, as Dr. Bagian said, what happened, why did it happen, and what are we going to do to fix it.

I would make another point which is that we still have out there a largely decentralized system. It is nonstandardized. There are not any simple fixes that we can plug in. Like with the blaster worm, you were able to put one fix in and put it across the system if you have a standardized system. But we do not have that, so there are not any simple fixes.

The other issue we have here is that for the most part, 190 some thousand of those 235,000 employees are in the veterans health arena and that is where we have the responsibility to deliver healthcare. And as I have testified before this Committee in many previous hearings, we have approached this from the start with the principle, "do no harm." Do no harm is a part of the way you have to approach this. We cannot afford to shut down a hospital system where patients are being taken care of.

Plus, we are a government agency. We deal with civil service rules. We deal with contracting rules, and we go forward with all those issues. So that is part of the explanation, sir.

Let me make the point, too, that I understand exactly where you are coming from and where the Committee is coming from, and it has been a long time. There are a number of issues out there. But as I said, we are working, and I think the centralization and reorganization of this office which the Secretary has directed will allow us to provide, in addition to what we had before, for education and information to be provided, that we use our VA Learning University as an additional effort to bring information and education to bear.

And the other part of it is the inspection part goes forward where we have just started inspections, some announced, some unannounced, to be able to go out and find out what is going on out there so we are not surprised.

Mr. MITCHELL. Just a quick followup. You mentioned your study and you are looking at why people do the things they do. When do you expect this study to be over? When do you expect to finally implement all of these recommendations? How long is it going to take?

Mr. MANSFIELD. Sir, I cannot give you a final date right now. I am sorry. I wish I could. I wish I could tell you that we have got this problem solved. We cannot do it.

As I indicated and as Secretary Howard indicated and as I believe Dr. Bagian indicated, it is a continuous ongoing effort where we are going to have to continue to work on all the different issues until we know that we have got every single part of this understood and we have got a fix prepared for it. We put the fix in and we make it work.

The final word I would say here is again that it is not a question of technology or machines or software. It is a question of people.

And we are going to be dealing with people across this system, the 235,000 employees, the tens of thousands of contractors, all the people in the 105 medical schools that we deal with where you have residents and interns in the thousands coming in and going out of our system every year. So we are going to have to work on this continuously, sir.

Mr. MITCHELL. Thank you.

One last question before I call on the Ranking Member. Mr. Howard, how long will the VA be without a cyber security chief?

Mr. HOWARD. Sir, we actually had selected one, a female, very well-qualified. We had selected her. Several days before she was to show up, she decided to take another job. So I have now had to go back through and announce that position over again. I assure you we will move as fast as we can. But the process has to be done correctly.

Mr. MITCHELL. Thank you.

Ms. Brown-Waite.

Ms. BROWN-WAITE. Thank you, Mr. Chairman.

You know, maybe reducing this to parenthood might be relevant because I only have two children that I gave birth to. One you could talk to and reason with and you would get results. The other one, it was like sometimes you had to like look her eyeball to eyeball and threaten sincerely in order to get her attention.

So I want to know what you are doing to really get the attention in this culture of where we did it before, so we are going to continue to do it, and I want to know also what is the VA's policy on using personal computers, i.e., you know, maybe a thumb drive and taking it home and working at home? And what happens to the employee who you might have to like take drastic steps to get their attention, i.e., dismiss them? Tell me what is going on because it is very frustrating to see the lack of progress here.

Mr. Mansfield.

Mr. MANSFIELD. Let me start with the last question, and that is the area of sanctions. And I think to approach that we have to understand that, as Dr. Bagian mentioned, that that is a part of a total spectrum of changing the culture.

When you are talking about sanctions, I think you have to start with what are our responsibilities before you can get there, and that is I believe that you need to let the people know what you expect of them, why you expect that, give them a chance to ask questions if they have questions about what is expected, and then go forward from there.

The second part of that is I think that you cannot have one single decision. You have to take each case, each individual and each situation in and of itself and you have to measure what happened in that case, why it happened, and perhaps what the results are.

Ms. BROWN-WAITE. Sir, with all due respect, we are talking about thousands, hundreds of thousands of veterans whose information is just out there.

Mr. MANSFIELD. Well, I understand that. I would tell you, Ms. Brown-Waite, that the last time I was admitted to a VA facility, which was not too long ago, one of the forms they gave me said you can check off up here, is this information available for VA research.

So I understand that every veteran in this system is at risk, and I hope the point is coming across that we are attempting to do everything we can to make sure that that risk is mitigated, if not eliminated.

Ms. BROWN-WAITE. Do you have written policies that say one time and one time only, if it happens again, you are out, or is it no strikes and you are out? What is VA's policy at this point on taking a risk with individuals' information that may put it at risk outside of the premises of the VA offices and hospitals?

Mr. MANSFIELD. Well, let me caution that, as I mentioned before, we live within the civil service rules and we have to recognize those and go forward and ensure that we carry out all the responsibilities we have there and ensure that each and every employee's personal rights are protected or else whatever we do is going to be overturned by an oversight body.

And the other point again is that I think we have to take each case in itself and look at what are the issues involved here, how much harm was involved, and exactly how egregious or, as you mentioned, repetitive was the issue, and go forward from there. And we cannot just put it down simply as these three issues or these rules apply to each and every situation. We have to look at what the individual situation is and go from there.

Ms. BROWN-WAITE. Sir, I have more concern for the employees and the veterans' information that is out there. That worries me. Put something in writing that is distributed to the employees that at least they will know exactly what the ground rules are. You take the stuff off campus and you have violated a rule. You are put on probation. It does not happen again. Put it in writing some place.

Let me get to the specific Birmingham issue. I have a large number of seniors and I have the highest number of people on Social Security and Medicare. Should I be alerting citizens that their doctors' information on that patient may also have been compromised in the Birmingham breach or are you doing it? What are we doing to protect not just the veterans but people who are on Medicare and Medicaid?

Mr. MANSFIELD. We are following through with the requirements the previous legislation referred to. Part of what we have to do there is a risk analysis, and our initial attempt was to have the IG do it. The IG just last week informed me that they do not believe they have the capabilities to do it. They also have raised some legal issues.

I brought that issue of risk analysis to the President's Identity Task Force at their last meeting, and we are moving forward in an attempt to find some, as required by the law, independent body to do the analysis in order to make a determination of who to notify in that case.

I would make the point, too, that I have seen some reports that talk about 1.3 million physicians. That is not the correct number. What was it, 196, I think we are down to?

Mr. HOWARD. Sir, 565 that we think are——

Mr. MANSFIELD. Why don't you——

Mr. HOWARD. To just comment a bit more on the list of providers, in the case of Birmingham, there were 1.3 million on the list. A large number were deceased. I believe several hundred thousand.

But in every case, we believe two elements of information were on the particular piece of data, name and date of birth. That concerns us obviously.

But the most critical was a population of about 565,000 where there also appeared a number not identified as such, but it happened to be a Social Security number. And so in the case of the 1.3 million providers, that is where we have pursued an official risk analysis on that to get specific guidance on how to approach it as the Deputy mentioned.

Mr. MANSFIELD. Let me just clarify that the providers are not all medical doctors.

Mr. HOWARD. They are not all medical doctors. Some are nurses. There is a variety of providers on the list.

Ms. BROWN-WAITE. But, sir, it is very easy—and I would ask the Chairman's indulgence——

Mr. MITCHELL. Yes.

Ms. BROWN-WAITE [continuing]. It is so easy, once you have a provider number, to engage in Medicare and Medicaid fraud. It is out there. And, you know, I do not know how long your risk analysis is going to take. You know, the frustration that I have is that we have people's identities and medical information and Social Security numbers. Now we have physicians' information also at risk.

And the ability of somebody to go in and set up a post office box and do Medicare or Medicaid fraud, that is a dangerous situation.

Mr. MANSFIELD. I fully agree with you and understand it. I would make the point that it has taken us a number of days to do the analysis that the OIT Office has done to find out who has been on those records and how many names there actually are and who they are and what information is attached to that in an effort to go forward and find out what we have to do to answer the questions you raise which are so important.

Ms. BROWN-WAITE. One last question. I promise this will be the last. Do you have a breakdown by State of the providers and have they been even notified of this, because I will tell you, nothing will send a more chilling effect to a physician or another healthcare provider if they think somebody may be out there billing in their name because once CMS gets on their case, you cannot get them off?

Mr. MANSFIELD. We do not now have the addresses. The file that we obtained from CMS was scrubbed down to a certain degree, they thought including removing of Social Security numbers, and that means that we are going to have to go back because when we get the full identity of the individuals to CMS and get them to provide us the addresses as we go forward in notifications.

Ms. BROWN-WAITE. Thank you, Mr. Chairman. I am sorry.

Mr. MITCHELL. That is fine.

Mr. Stearns, I understand you have to leave immediately.

Mr. STEARNS. Well, not immediately. Can I follow up on my colleague's—what I had is something that follows right after my colleague.

My colleague from Florida mentioned this Unique Provider Number (UPN). Tell me what that means. She touched on it, but from your perspective, what does that mean for a person, a lay person?

Tell me the significance if a doctor had their unique provider number.

Mr. MANSFIELD. Sir, Mr. Howard has been working with these files, and I will let him explain what the UPN is.

Mr. HOWARD. Sir, it is an identifier, you know, for the physician. Quite frankly, though, it is the presence of that Social Security number that is probably even more critical.

Mr. STEARNS. If you had the UPN number plus the Social Security number, does it give you authenticity and credibility, or if you just had the UPN number without it, you would not have it?

Mr. HOWARD. Sir, I do not believe the UPN number alone would provide you what you need to set up a fraudulent situation on Medicare. But I might ask——

Mr. STEARNS. Are you absolutely sure that if I sent HEAD some fake stationery and I used a UPN number, could I not start billing for Medicare based upon that without a Social Security number? Yes or no? If you do not know, just say you do not.

Mr. HOWARD. I am not sure, sir. The information I have, that is not enough, but I am not a physician.

Mr. STEARNS. Because in addition to the loss of personal identifiable information which means we have hurt the identity of veterans as well as physicians and physician providers, you have another avenue here of fraud dealing with the Medicare program which we did not have. When we had 26 million veterans, we were worried about loss of personal information. But now having compounded on this, what I hear from my colleague and this UPN is that the possibility could be you take this information and forget trying to steal a person's personal information. Just go to the source and start billing Medicare for thousands and thousands of dollars. And do it from 50 states before you get caught, you could collect a lot of money. Am I exaggerating or is that a possibility?

Mr. HOWARD. Sir, the UPN number, to my knowledge anyway, is publicly available. That is why I say you would need more information to actually set up a successful——

Mr. STEARNS. So I could find out the UPN number for my physician? It is accessible. Okay.

Mr. MANSFIELD. Web site, right?

Mr. HOWARD. It is on a Web site.

Mr. STEARNS. It is on a Web site. So that is not critical information. Okay.

Mr. HOWARD. No, sir.

Mr. STEARNS. Okay. The gentle lady, I will yield to her if you have any additional—go ahead. I am just going to yield a minute to her.

Ms. BROWN-WAITE. What I said to my colleague is the provider number, the Medicare provider number is something that they would need to set up a storefront and start billing, because we had exactly that problem in Florida.

Mr. STEARNS. Right. And that was part of the loss of 1.3 million, right, what she is talking about.

The other thing I cannot understand, this occurred on January 22nd. Why have you not given Members of Congress or at least put a profile of this information by State? I mean, at what point are you going to decide to notify these people?

In California, there is a law that once you lose this information, you have got to notify the people immediately. How long are you going to take and why have you not come up with a plan and a date when you are going to do this? Are you just going to wait until you get it back, which might be 6 months? It seems to me there is a time where people should be notified that you have compromised their personal identifiable information.

Mr. MANSFIELD. Let me make the point, sir, that since we became aware of this, we have been in communications with CMS and talking to them and their legal people and others in an effort to determine what we need to do to go forward.

I would also make the point that it has been a question of attempting to find out what the information was because it does not show up as a Social Security number. It is in a box over here that has a name on it and it took our people a lot of work to——

Mr. STEARNS. So you have to go in each individual box for a name to find it?

Mr. MANSFIELD. You have to go through that to find out, you know, if that number matches a Social Security number, we believe. And we have had to go back and do the forensic information to get that. That has taken some time.

And I would make the point that we frankly concentrated on the veterans in an effort to get them identified and to get the notifications to them. We are continuing to go through the process of pulling all these large files together to get those names of the veterans and to notify them.

Mr. STEARNS. In any corporation, they have a security protocol which says that only certain individuals get access to this information. I cannot understand why your agency has not developed a protocol so that this veteran would not get access to that.

And the second question I have and I will complete is CMS, are they not derelict for giving you access to this information without it being encrypted? Shouldn't CMS at the very least encrypt all this information before so that this person that you put on the protocol would have a password and either an iris or a fingerprint before he or she could get this information?

So my two questions are, is there not some culpability on CMS for not encrypting and, two, why do you not have some kind of protocol with that massive information?

Mr. MANSFIELD. Sir, part of the problem is that this list was available for our medical researchers under a memorandum of understanding that we had with CMS. And actually my understanding is that they gave us the wrong list that was put into the custody of a person that we had responsible for receiving that and responsible for making the decision to release it to the proper people who have authority and permission to be released to.

In the process of looking at the list that we got, we found out that there was more information, including Social Security numbers, that were on there and identified as such and we got those removed from it. But we did not realize that this other number potentially could be a Social Security number also. So that is part of the problem.

Mr. STEARNS. Thank you, Mr. Chairman.

Mr. MITCHELL. Thank you.

Mr. Walz.

Mr. WALZ. Thank you, Mr. Chairman.

Once again, Mr. Mansfield and the panel, I do not intend to bore you with my personal history. But having been one of those veterans who lost their data in the first breach and having received the letter, I give it to you more as a person at the time who was not in Congress but who was a veteran and got the letter and got notification on the news that this happened and watched this unfold.

And it was very damaging because the first thing it did it made me lose some faith in the credibility of the VA. That was really critical to me because I want to believe and, as I said in the beginning in my opening statements, your intentions are unquestionable. You are there to serve our veterans. You have done that.

But when I am listening to my colleagues and I listen to what is coming out on this, outcomes matter more than intentions. There is no doubt about that. And as a veteran, I know my first instinct was just get this right, whatever it takes to get this right.

And I hear you say, you talked about, well, you have got civil service issues and contracting issues and things like that. Dr. Bagian was talking about, and I am sure you did, your organizational analysis and you went through, you know, gap analysis or whatever you did.

If you were given free reign—this may be more hypothetical, but maybe it gets to where we need to get with this—what are these constraints that are stopping you from getting this fixed? When I hear you say you have these civil service contracting issues and so forth, what would you change if you were unrestrained by those? What would fix it?

Mr. MANSFIELD. Sir, I have to make the point that, you know, I come down here as a representative of the Administration, and there are some other constraints that apply also.

Let me go as far as I can and push up against the fence. One of the constraints we have with this reorganization to make sure that we shrink down the amount of responsibility so the people in those boxes can actually get their hands around it and do it instead of having too much to do, which I think we had previously, is to change the law that is set up at the Department of Veterans Affairs as a cabinet agency, because IBM, a respected contractor that came in to help us figure out what this reorganization could be, said that some of those positions should be Deputy Assistant Secretaries in order to get the people that we want to get that maybe took another job because they had a better offer.

And the law that established this Department established a number of Assistant Secretaries and then put a ratio of Deputy Assistant Secretaries. The IBM recommendation is that we have a significantly larger amount of Deputy Assistant Secretaries.

So I would ask you to amend the law. That is an issue that we have to deal with, and I am trying to answer your question and again play by the rules.

Mr. WALZ. I appreciate your candidness.

Mr. MANSFIELD. The other issue is that we have a limited number of SES positions. And when the 4,600 people were transferred

in here from the field to put together an organization, how many SES positions were transferred in?

Mr. HOWARD. None with those transfers.

Mr. MANSFIELD. None. So that is an issue that we are dealing with, and that means that in my responsibility to allocate those positions across the Department, I have to pluck them from somewhere else, which I have done, but there are more requests for that on the table too. And we have to go through things like that. So that means we are going back to OPM and trying to get that number raised up.

And then the other part is as the Assistant Secretary indicated, with this person that was hopefully going to be in the job out of the picture, then we have to go back and what, do we have to post it again?

Mr. HOWARD. Uh-huh.

Mr. MANSFIELD. So we have to go through a long, lengthy process that just is there. I am making the point. We live by those rules, and those rules were put in place and that is the law and those are the regulations. We live by them and we try and, you know, push as far as we can on those, but there are restrictions involved here.

Mr. WALZ. Well, I appreciate your candor, and I will finish up on my last bit of time here.

Are you optimistic inside the parameters you have to operate it that we can get security on this data? Can we get this done or are we simply chasing after our tails on this because of the parameters that are put on you and we are never going to get there?

Mr. MANSFIELD. We will get it done, sir. We will get it done. The problem we have is time and people. We can work with the people. We can do a better job of educating them. We can make sure they understand what they need to do. We can follow Ms. Brown-Waite's suggestion and make sure they understand if they do a wrong, then there are sanctions available.

But we have got 235,000 individuals out there and we have got tens of thousands of contractors and every June, we have got how many thousand residents and interns coming in the door?

Mr. HOWARD. Tens of thousands.

Mr. MANSFIELD. Tens of thousands there, so we have got to go through that. I wish I could tell you we could line everyone up and zap them and it would take place.

Mr. WALZ. Thanks, Mr. Mansfield.

Thank you, Mr. Chairman.

Mr. MITCHELL. Thank you.

Mr. Rodriguez.

Mr. RODRIGUEZ. Mr. Chairman, if I could follow-up on the same, if it is okay.

What I am getting and what I am seeing is a bureaucratic nightmare, and I can just assume in terms of what you are having to go through. So I am thinking you almost need an external group coming in, you know, in terms of cyber security to go in there and take care of it for you.

You say no, but, my God, you almost need someone, a task force to deal with it and come and tell you where the gaps are and what

you need to do that is external from you to be able to tell them how to protect that.

And I am just going to share with you, you know, I was engaged in one of the few exercises prior to 2000 on that glitch referred to as dark screen out of San Antonio. And as a result of that, there is a whole group, you know, and I think Senator Hutchinson and them came up with—because we did not have enough people in cyber security—they came up with a Master's Degree there. And there is a group there that has been going around the country helping both the private sector and the public sector on cyber security. And, you know, you almost need somebody in all honesty because you have got to pull this off as quickly as possible, and they can tell you where the gaps are. They can tell you what you need to do. They could even tell you that they can break into it now or not.

And so, I hate to do something like that but I think that that would be something that is probably almost needed where you need an external task force to come in there and take care of it. And I think that would really be helpful not only to you, but to all the veterans that you are serving, because I know that you are sincere about wanting to do that.

But I also sense your frustration and the fact that in some areas, you are having some—you know, look at that chart. My God, you have got a mess. And so you need an external group to come in there and tell you gaps that you are probably not aware of that you already have and how to correct it.

Mr. MANSFIELD. Well, sir, I would agree with you and make the point that in the process of getting to here, we did that. As a part of the reorganization, we brought in IBM and we brought in subsidiary contractors under that, and they came up with many of the recommendations from an outside view looking at our system, taking a chance to go around and look at it and help us understand what we needed to do. And part of that chart that you see there is as a result of that. Also some of the processes and policies that we need to put in place were recommended by them.

Mr. RODRIGUEZ. Mr. Chairman, I apologize. I would presume that if this continues, I would ask if maybe there is some way that as a Committee, we can force an external group to go in there as a task force to look at the whole—and people that are trained in cyber security to protect the agencies and to protect the Department of Energy.

There are groups out there, because we get hit, you know, through cyber space. And those same people that hit us are real good at also being able to protect us, but also learn where the gaps are at. And at some point in time when the agency continues to have difficulty that we take that into consideration.

Mr. STEARNS. Will the gentleman yield?

Mr. RODRIGUEZ. Yes, sir.

Mr. STEARNS. I think your suggestion is excellent. And the GAO has made recommendations since 1998, 150 recommendations, and they have not been implemented. Even their Inspector General of the Veterans, there are 16 recommendations from 2004 that have not been implemented. So I think your idea is absolutely on target that we need to have an outside group.

And there are outside agencies, like accounting firms, that went in and checked Enron. You could have these outside security firms go in there and give you the information you want. And right now they have thousands of computers they have not even inventoried or encrypted. So I think your suggestion is right on target.

Mr. RODRIGUEZ. Thank you.

Mr. MITCHELL. Just one comment that I think will help everyone. Looking at this chart, I can see why things are not really moving, because no one up here can read it. I do not think anybody can.

And I would suggest next time that you bring a picture chart and also provide all the Members with a chart because I have no idea what that says. I can see, I think, it is yellow and blue and white boxes, but that is it. So I would suggest that next time you make a presentation like that that you provide us all with——

Mr. HOWARD. Mr. Chairman, we have——

Mr. MITCHELL. That would be nice.

Mr. MANSFIELD. Secretary Howard mentioned in his comments that if you want to discuss it that we would go forward and do that. I apologize for——

Mr. MITCHELL. You keep referring to it, so I assume you wanted us to be able to see it.

Mr. MANSFIELD. Yes, sir.

Mr. MITCHELL. Mr. Rodriguez.

Mr. RODRIGUEZ. Yeah. One last comment. And I sense you are sincere in terms of wanting to do the right thing. But I also pick up in terms of the fact that I am sure there is some frustration on your part in terms of trying to accomplish what you need to get done. And so with that, I will stop.

Mr. MITCHELL. Thank you.

Mr. Davis.

Mr. DAVIS. Thank you, Chairman, for letting me participate again.

Mr. Mansfield, let me use March 2006 as the trigger for this question. That was, as I understand it, the time in which there was a fairly significant data security breach at the VA. Have I got the timeframe right, March 2006?

Mr. MANSFIELD. Sir, it was May of 2006.

Mr. DAVIS. May 2006. Since May 2006, how many data breaches are believed to have occurred at VA facilities?

Mr. MANSFIELD. Sir, I can tell you that from the SOC report that we get, and I do not have a number with me, I will provide that to you as a followup to this hearing, but we know that there have been hundreds of them in the sense of actual violations of either the law or the regulations.

Mr. DAVIS. And you mean hundreds just in that timeframe since May of 2006?

Mr. MANSFIELD. Yes, sir. Since we put this new SOC reporting system into place following the May incident.

Mr. DAVIS. What would you estimate the largest amount of information that has been compromised in any of those hundreds of breaches?

Mr. MANSFIELD. How many were in the——

Mr. HOWARD. It was Birmingham.

Mr. MANSFIELD. I think the Birmingham incident where we are talking about——

Mr. HOWARD. It is number two.

Mr. MANSFIELD [continuing]. Is the second one, approximately a half a million veterans and approximately the same number of providers.

Mr. DAVIS. Well, give me a general estimate in what you describe as the hundreds of breaches that have happened since May of 2006. Give me an estimate of the amount of information that you think has been compromised collectively.

Mr. MANSFIELD. Again, sir, let me go back for the record. Some of these reports involve two veterans' information or——

Mr. DAVIS. That is what I am asking you. I understand that.

Mr. MANSFIELD. Yeah. I mean, I do not have that in front of me. Well, I can get it and have it provided for you.

Mr. DAVIS. I am certainly not empowered to make requests on behalf of the Committee, but I suspect the Committee would be interested in having that information, and leads to my next question.

Mr. MITCHELL. Absolutely.

Mr. DAVIS. Other than the Birmingham breach, how many of these breaches have resulted in a public notification?

Mr. MANSFIELD. The UNISYS?

Mr. HOWARD. Sir, let us get back to you on that. There have been a number of them. But to give you a precise answer, we need to go back and check.

Mr. DAVIS. Mr. Mansfield?

Mr. MANSFIELD. I would just make the point that in some cases, there has been lower numbers here. The veterans have been notified that or possibly also employees that might have been identified, but not necessarily the public. So we have to go back again and sift through all that and then followup. Many of these decisions can be made at the facility level.

Mr. DAVIS. Is it safe to say that the Birmingham incident is the only instance in which a press release has gone out from the VA notifying the public of a breach since May 2006?

Mr. MANSFIELD. No, sir.

Mr. DAVIS. How many other times has a press release gone out notifying the public?

Mr. MANSFIELD. I will have to go back and check. I do know on the UNISYS, there were a number of press releases. That was the one where one of our contractors—I am not sure how many——

Mr. DAVIS. That leads to my next set of questions. I do not get a sense that there is a hard and fast policy regarding when you notify, when your agency notifies and when you do not. Can you give me a short, quick sense of what is the trigger, when do you all engage in public notification?

Mr. MANSFIELD. It is a combination of events. I think at——

Mr. DAVIS. Is there a statute you can point me to or regulation that you can point me to by number?

Mr. MANSFIELD. I am going to have to go to my general counsel, sir. I cannot point to a statute.

Mr. DAVIS. Let me ask the general counsel. I am seeing if there is a particular place that contains the relevant policy.

Mr. MANSFIELD. Well, I think again, it becomes a question of what is the size of the event, what is the information given out. In some cases, it may be that there is incorrect information given out in the press and there may be an attempt to try and correct that.

Let me also make the point that in any serious breach where the IG moves in and accepts the responsibility to go forward with a recommendation, they generally request us not to make any public notification.

Mr. DAVIS. Let me ask you about that, Mr. Mansfield. And to me, that is one of the major problems here. I understand that there was a request from the IG, wait, let us do a more thorough investigation. I understand that at some level, but here is the problem. Every moment of delay is a moment in which information can be compromised. Every moment of delay is a moment in which information can be misused or misbilled. And it would seem to me that the balance would err in favor of notification, and that does not appear to be where the balance was in this case. Am I wrong?

Mr. MANSFIELD. I will not say that you are wrong, sir. I will say that——

Mr. DAVIS. Why shouldn't the benefit of the doubt be given to the veteran?

Mr. MANSFIELD. Part of it is, sir, in those early instances—for example, in this case, we did not have the information available to go notify the veterans or know how many veterans there were actually involved or know who they were and where they were and how we can get in touch with them.

Mr. DAVIS. Once you got that information, did notification occur?

Mr. MANSFIELD. Yes, sir.

Mr. DAVIS. Well, I am not sure if that is accurate, but let me move on if the Chair would indulge me to have just a few more seconds here.

You made a reference in your opening statement to the Birmingham facility, and I looked for your written statement and I did not find a reference characterizing the conduct or the performance of the Birmingham facility.

So let me ask you. Would you grade for me the Birmingham facility with respect to its handling of this matter? Would you give them an assessment or grade?

Mr. MANSFIELD. Well, obviously with the problem that we have here, there is some concern about what happened. I am still waiting for the IG to hand me an investigative report.

Mr. DAVIS. What is the nature of the concern? I understand there is an individual who is compromised, and I do not want to get into the details of that if there is an ongoing investigation. But beyond that individual, would you assess the performance of the VA in Birmingham?

Mr. MANSFIELD. No, sir. I am not going to do that now.

Mr. DAVIS. And the reason?

Mr. MANSFIELD. I would be happy to go off line and away from the domain here and have a conversation.

Mr. DAVIS. Is that not a matter relevant to the public? What is your position, sir?

Mr. MANSFIELD. I am trying to follow the directions and orders that I have and perform the job that I am supposed to perform for

my boss, who is the Secretary of the Department of Veterans Affairs, and allow him the ability to make what decisions he has to make in the proper forum.

Mr. DAVIS. Mr. Chairman, I am sensing the fact that my time is out. If I can just wrap up with one observation.

I am concerned by that answer, Mr. Mansfield, because this is the people's business. This is the ultimate public domain, a congressional hearing, and if it is the assessment of senior management at the VA that the Birmingham facility is not meeting its obligations with respect to data security or some other aspect of this matter, I would like my constituents in Birmingham to know that and I think that that is not a privileged matter. It is not a matter of national security. It is something they are entitled to know.

Mr. MANSFIELD. When that decision is made, sir, I will make sure that I let you know and that we let the people know. And I would state for the record that notification of veterans started on 5 February of 2007.

Mr. MITCHELL. Thank you.

Before I call on Mr. Bachus, I was just made aware that Public Law 109–461 enacted in December of 2006 permits the Secretary of the Veterans Administration to determine when to announce and make public any information of this kind.

Mr. Bachus.

Mr. BACHUS. Thank you.

Mr. Mansfield or Secretary Mansfield, my father was a veteran who was treated at the VA facility. He is now deceased, but my mother received notification that his records were among those lost.

And I will tell you if he were here today, the first thing he would say is thank you for the medical care he received at the VA hospital. It was first rate. He had Alzheimer's, and he had the veterans facility there, partners with the UAB Medical Center, and he received medical care that was second to none.

Mr. MANSFIELD. Thank you for those comments, sir.

Mr. BACHUS. Wonderful staff there. Y.C. Parris, I see is on the third panel. It is a wonderful staff. So I do think, to put this in perspective, this is one employee. Did he violate a VA written rule? I mean, is there——

Mr. MANSFIELD. The individual that reported the incident and——

Mr. BACHUS. Yes.

Mr. MANSFIELD. Yes.

Mr. BACHUS. What has been reported is he downloaded the entire system on a hard drive and then took the hard drive off premises; is that correct?

Mr. MANSFIELD. Yes. And the rules state that you can do that, but to do it, you need your supervisor's permission and they have to be encrypted.

And the original report we received through the SOC, we were told that the numbers were less than eventually turned out to be true. I think he reported somewhere around 48,000 to 56,000 and reported that the information had been encrypted.

But when the forensic people from the FBI with the IG went in and did the forensic examination, that is when we started to find

out that we had these mega numbers involved in the—potentially had these—we still do not know what they are, but potentially had these mega numbers involved.

Mr. BACHUS. You know, I think maybe a problem may be what is the policy on either downloading information on a hard drive or thumb devices and then walking out of the VA with those devices. To me, there ought to be a pretty firm rule that you do not do that or that all information is encrypted.

Mr. MANSFIELD. That is the current status in Directive 6504 which has been published as a followup to the May incident. There is a requirement, as I stated, to get permission and then have it encrypted.

Mr. BACHUS. You know, this Committee, I am not on the Committee, but they receive a weekly update on any security breaches, and one of those breaches that they received was an instance where a staff member was checking software on various machines at a VA facility and found that many of the workstations were logged on. There was no one at the desk and they had not logged out. And you could take that computer and go into the entire NT system. Is that a violation of the rules?

Mr. MANSFIELD. Yes, that is, sir. When that station is not being used, it has to be shut down.

Mr. BACHUS. There are no locks in place?

Mr. MANSFIELD. There are time-outs where, you know, after a certain period of time, and I do not know exactly on those machines you are referring to, but that the machine will shut itself down. That is a new thing we have——

Mr. BACHUS. Yeah. The person involved here was actually a computer programmer, was it not?

Mr. MANSFIELD. I am not sure which one you are referring to.

Mr. BACHUS. In Birmingham.

Mr. MANSFIELD. Oh, I am sorry. Yeah. In that incident, yes.

Mr. BACHUS. I am sorry. I did confuse you.

Mr. MANSFIELD. Yes, you are right, that was the person that we are talking about. It was a status 2210 computer.

Mr. BACHUS. So he certainly knew the risk involved.

Mr. MANSFIELD. He reported the issue because he knew that, you know, there was a problem. There are other issues that apply to it too that——

Mr. BACHUS. Was it not in the report that it was lost off premises though?

Mr. MANSFIELD. Actually, I just know that it was reported lost.

Mr. BACHUS. I will say this. The day that the VA in Birmingham discovered it, they notified the IG, which was the next, you know——

Mr. MANSFIELD. They notified the SOC, which is us, and we notified the IG.

Mr. BACHUS. I am sorry. The SOC. So their notification to you was immediate?

Mr. MANSFIELD. Well, yes.

Mr. BACHUS. One last question, if I could. The thing that probably disturbs me that I heard today that, you know, of course, you shared it with us February 9th, which you asked us not to make it public, you know, obviously has come out in this hearing.

Is the 1.3 million medical health providers, and it is not all doctors—I know some are dead, but most are alive and, you know, therapist, anyone that bills the VA basically is what we are talking about here, is that right, or does research for the VA or medical care, 1.3 million healthcare providers?

Mr. MANSFIELD. Excuse me. Could you restate that? Is the question, are any of those private providers people that would bill the VA?

Mr. BACHUS. Yeah.

Mr. MANSFIELD. Potentially could.

Mr. BACHUS. No. I mean, is it——

Mr. MANSFIELD. I mean, I do not know, but potentially they could be.

Mr. BACHUS. Okay. Well, now, the physicians, I will just say that, you know, was it their names were on there, their date of birth, their credentials also, right?

Mr. MANSFIELD. Their specialties, yes, sir.

Mr. BACHUS. Their specialties. The schools they studied at were on there?

Mr. MANSFIELD. I am sorry, sir?

Mr. BACHUS. The schools they studied at would have been on there because that is the HHS form, is that correct?

Mr. MANSFIELD. Sir, we will double check for you, sir. I believe that you are right.

Mr. BACHUS. Yeah. Yeah, the form that you have identified as being the HHS form has the school they studied at, their provider numbers, their billings, license. And somebody mentioned a medical license number. That is a tremendous amount of information.

Mr. MANSFIELD. I think that may be the M link number which again is potentially another number.

Mr. BACHUS. Okay. All right.

Mr. HOWARD. The school they graduated from is also on there, sir.

Mr. BACHUS. What?

Mr. HOWARD. The school they graduated from——

Mr. BACHUS. Where they graduated medical school.

Mr. HOWARD. We have a picture we can actually show you.

Mr. BACHUS. And I actually have pulled up what is on that HHS—it is HHS information. But you mentioned a medical license. Is that different? What is the medical license? Is their medical license number included there?

Mr. HOWARD. Are you referring to the M link?

Mr. BACHUS. No. I do not know. Someone in this hearing mentioned the word medical license.

Mr. HOWARD. State license, yes.

Mr. BACHUS. Oh, okay. Their State medical license. Okay. All right.

Mr. STEARNS. Is it medical license number?

Mr. BACHUS. Yeah, their number, their license or State license. Okay. Now, the provider numbers, their billing licenses is all on there?

Mr. MANSFIELD. No.

Mr. HOWARD. I do not see it.

Mr. BACHUS. Okay. All right. You know, all that information surely puts them at very high risk for Medicare billing fraud. I mean, someone else could bill for their services. But what I am hearing today is that they have not been notified?

Mr. MANSFIELD. Sir, not yet, sir. We are still trying to identify. Much of this information is available to the general public on other Web sites, too, also. So we are trying to figure out what additional risk do we have to deal with here based on what information is provided on this document.

Mr. BACHUS. But now, I guess you could not go publicly. Could you go in and get all that including their Social Security numbers and their billing license, their provider numbers?

Mr. MANSFIELD. Go ahead.

Mr. BACHUS. I would hope that is not public.

Mr. MANSFIELD. I would ask General Howard to answer that question, sir.

Mr. HOWARD. Sir, in the case of physicians, the name and date of birth, in fact, the date of birth of physicians can be found on Web sites. For the other providers, that may not be the case. So in the case of physicians, there is at least two items of information that we would consider sensitive that is available, you know, the name and the date of birth.

Mr. BACHUS. And I guess it begs the question. I will end with this. As a result of that, you have got all this disclosure out there. And I do not know whether it has fallen into anyone else's hands or not, but it seems like at least one question you might be asking is do you change these numbers in the national system. But I know you are in touch with CMS, but have there been any reports of any fraudulent billings?

Mr. MANSFIELD. No, sir, not to our knowledge.

Mr. BACHUS. Thank you.

Mr. MITCHELL. Thank you.

There are two people who said they wanted a followup question real quickly.

Mr. Stearns, did you want to have a followup very quickly and then Mr. Davis, and then we are going to take a 5-minute break?

Mr. STEARNS. My colleague, Mr. Bachus, had mentioned that he is concerned about fraud. And, Mr. Chairman, the only thing I think, you cannot get all that information in one fell swoop like that.

And it seems to me that you have got to make an assessment here for CMS and the veterans of the degree of fraud that could be instigated because you have all this information. You would set up a dummy office as well as stationery and you could say I am billing for John Miller, a followup, because you obviously can send with all this information and how would Medicare not know if you put together a bill and sent it forward? Why would Medicare not pay it with all that information available?

So I think there is a danger of loss of personal identifiable information for veterans, but also you have a possibility of fraud on CMS. And that is just an area that I think somehow you have got to get a handle on. And I am not sure except one of my colleagues suggested having an expert outside auditing firm come in and help

you assess the risk as well as to try and implement some procedures.

Thank you, Mr. Chairman.

Mr. MANSFIELD. That is, as I mentioned, sir, a requirement of the statute and does require independent analysis. We have a responsibility within 180 days of passage of the law to write the regulation that would make that work since we do not have that regulation written yet. We are in the process, as I indicated, in discussions with CMS, CMS lawyers, and how do we go forward in attempting to do that.

And I would make the point that, as mentioned earlier, that we do have to be—we have had discussions, many discussions about this, and we do have to be aware and we do have to take it very seriously. But part of the problem is, you know, we have been working on the effort to identify whose identities actually are in there and, you know, as mentioned, which ones are alive and then exactly how many are physicians versus other providers. And then we have to do a process to get the addresses if we go forward. So we are working on these issues internally.

Mr. STEARNS. One other thing I would caution you about is I understand you have not done a full audit of all your computers and you have not instigated an encryption procedure.

So, you know, the staff showed me you have had other incidents of loss or breach of information and it is going to continue to happen unless you get a handle on this which means you have got to complete your audit on these computers, you have got to put encryption protocol that I mentioned, or you are going to have this on your watch again and again.

Mr. MANSFIELD. As I mentioned earlier, we are aware of that, sir. And as I mentioned earlier that with a decentralized system that we have and the fact that we are not standardized, we do need to move toward standardization, that there are not any simple fixes that allow us to just punch in the answer and go forward.

We have to make sure in each of the many very different systems that we have across the VA, across all these hospitals and healthcare systems, that it is going to work and not shut down a system. And it is a lot more involved than I understood it was when we started this. And we are going forward as fast as we can to make sure that we get it done. But, again, the lead word is still do no harm and make sure that we get the veterans that are coming in for treatment treated and taken care of.

Mr. MITCHELL. Thank you.

Mr. Davis has one question, then Ms. Brown-Waite has one question. We want to get to the second panel.

Please ask the one question.

Mr. DAVIS. Thank you, Mr. Chairman.

Mr. Mansfield, with respect to the hundreds of breaches that you say have occurred since just May of 2006, has a single VA employee been fired or disciplined as a result of any of those breaches?

Mr. MANSFIELD. The answer I am told is yes, but let me, if I may, sir, go back and make a point. All these reports are not IT breaches. Some of them are paper records. Our Veterans Benefit Program is based on paper files of millions of veterans. Some of

them are based on paper records in other incidents. So they are not all IT.

Mr. DAVIS. Thank you.

Mr. MITCHELL. Ms. Brown-Waite.

Ms. BROWN-WAITE. A quick question about the cyber security person that you were going to hire. If you had, you know, narrowed it down to the top three or the top five and the one person declined, is there a reason why you cannot go back and look at the second person? Do you have to rebid this?

Mr. HOWARD. Yes. That is what the process is.

Ms. BROWN-WAITE. Thank you.

Thank you, Mr. Chairman.

Mr. MITCHELL. Thank you.

We are going to take a 5-minute recess and then have the second panel come up. Thank you.

Mr. MANSFIELD. Thank you, Mr. Chairman and Members.

[Recess.]

Mr. MITCHELL. All right. We will continue this Subcommittee hearing. I want to welcome panel number two. I welcome panel two to the witness table.

And these individuals provide our Subcommittee with a major service not only in their ability to provide independent assessments of VA program performances, the GAO and VA IG are able to place the performance of VA's information security management program in a historical context. This allows us to better understand if cultural resistance has developed in the program and how to cope with this resistance.

I have asked Mr. Claudio in his newly-created role in the Office of IT Oversight and Compliance to sit in on panel two and to answer our questions. That his position was recently created by the Secretary to provide a feedback mechanism with regard to the information security program is laudable. We are interested in his grass-roots viewpoint. And we will begin with Mr. Wilshusen.

STATEMENTS OF GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION TECHNOLOGY SECURITY ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; MAUREEN REGAN, COUNSELOR TO THE INSPECTOR GENERAL, OFFICE OF THE INSPECTOR GENERAL, U.S. DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY KENNETH SARDEGNA, DEPUTY ASSISTANT INSPECTOR GENERAL FOR AUDIT, OFFICE OF THE INSPECTOR GENERAL, U.S. DEPARTMENT OF VETERANS AFFAIRS; AND ARNALDO CLAUDIO, DIRECTOR OF OVERSIGHT AND COMPLIANCE, OFFICE OF INFORMATION TECHNOLOGY, U.S. DEPARTMENT OF VETERANS AFFAIRS

STATEMENT OF GREG WILSHUSEN

Mr. WILSHUSEN. Thank you very much, Chairman Mitchell, Ranking Member Brown-Waite, and Members of the Subcommittee. Thank you for inviting me today to participate in the hearing on information security management at the Department of Veterans Affairs.

Recent well-publicized security breaches at the Department have highlighted the importance of effective information security con-

trols in protecting sensitive and personal information not only at VA but throughout government.

As we have reported on many occasions, poor information security is a widespread problem that can have devastating consequences, such as disruption of critical operations and unauthorized disclosure of highly sensitive information.

Today I will discuss the recurring security weaknesses that have been reported at VA and the actions taken by the Department in response. I will also discuss our ongoing work at the Department.

Since 1998, GAO and the Inspector General have reported on wide-ranging deficiencies in the Department's information security controls, including a lack of effective control to prevent individuals from gaining unauthorized access to computer systems and sensitive data and to detect them if they do.

In addition, the Department had not consistently provided adequate physical security for its computer facilities, assigned duties in a manner that is segregated, incompatible functions, controlled changes to its operating systems, and updated and tested its contingency and disaster recovery plans.

These deficiencies existed in part because VA had not implemented key components of a comprehensive integrated information security program, including the lack of centralized management and approach for addressing security challenges.

VA has taken important steps to improve security, including realigning its security functions and personnel under the Department's CIO Office. It has also developed a data security corrective action plan that is to guide and track the Department's efforts in implementing its information security program and controls.

However, many of these efforts have not yet been implemented. For example, key policies such as those for assessing risk and implemented enterprise patch management have not yet been developed.

In addition, the Department has not established a track record of proactively mitigating known weaknesses across all of its systems. As a result, sensitive information remains vulnerable to inadvertent or deliberate misuse, loss, or improper disclosure as the breaches demonstrate, nor has the Department consistently satisfied the provisions of the "Federal Information Security Management Act" (FISMA).

OMB requires agencies to annually report on their progress implementing FISMA by October 1. Although it sent a draft report to OMB, the Department has not yet submitted its official annual report for 2006. It is the only one of the 24 "CFO Act" agencies that has not yet done so.

At the request of this Subcommittee and other congressional requesters, GAO is presently reviewing the Department's lessons learned on notifying officials and affected individuals on data breaches, actions to strengthen information security, inventory and accountability controls over IT equipment, and efforts in implementing the VA's IT realignment initiative. These reviews are ongoing and will be completed later this year.

In summary, longstanding control weaknesses at VA have placed its information systems and information at increased risk of misuse and unauthorized disclosure. Although VA has made progress in

mitigating previously reported weaknesses, it has not taken all the steps needed to address these serious issues. Only through strong leadership, sustained management commitment, and vigilant oversight can VA implement a comprehensive information security program that can effectively manage risk on an ongoing basis.

Mr. Chairman, this concludes my statement. I would be happy to answer questions.

Mr. MITCHELL. Thank you.

Ms. Regan.

[The statement of Gregory Wilshusen appears on pg. 63.]

STATEMENT OF MAUREEN REGAN

Ms. REGAN. Thank you.

I would like to have our full statement submitted for the record.

And before beginning, on behalf of the OIG I would like to second the Deputy Secretary's comments regarding Mr. Sistek's retirement or move from the Committee. We have really enjoyed working with him over the years, and we will miss him.

Mr. Chairman, Members of the Subcommittee, thank you for the opportunity to address OIG oversight efforts of the VA's information security program, its effectiveness, and the need for cultural change within VA.

To answer questions regarding these issues, I am joined by Ken Sardegna, our Deputy Assistant Inspector General for Auditing.

Issues related to information security are twofold. The first is the protection of sensitive information maintained on VA automated systems from unauthorized access. The second is whether individuals who are authorized access to sensitive information adequately protect it from loss, theft, or inappropriate disclosure.

Today I will highlight that there have been longstanding problems in VA with respect to protecting sensitive information that have not been fully addressed. Our FISMA audits have identified information security vulnerabilities every year since fiscal year 2001.

VA's efforts to address these vulnerabilities in a timely manner have been hampered by the magnitude of the problems and aging IT infrastructure and the lack of standardized IT systems throughout VA.

To address these vulnerabilities, we have recommended that VA pursue a more centralized approach to IT management, apply appropriate resources, and establish a clear chain of command to enforce internal controls and hold individuals accountable for not protecting information.

In our ongoing 2006 FISMA audit, we determined that all 17 recommendations cited in prior FISMA reports remained unimplemented. In addition to the 17 unimplemented recommendations, we anticipate identifying several new high-risk areas associated with certification and accreditation of VA systems, remote access, and access to sensitive information by non-VA employees. Until all matters are fully addressed, VA systems and VA data remain at risk.

The May 2006 theft of an employee's personal hard drive containing protected information on at least 26 million veterans and active military highlighted how vulnerable VA is to compromising information on veterans.

In reviewing how this incident occurred, we found a patchwork of policies that were fragmented and difficult to locate. None of the policies prohibited removal of protected information from the work site or storing protected information on personally owned computers. These policies also did not provide safeguards for electronic data stored on portable media, such as laptops.

We also found information provided to VA employees and contractors needed to be better safeguarded. Background investigations were not always required or done. Procedures for reporting potential data losses needed to be improved. We made five recommendations to VA to correct these problems. To date, all five recommendations remain open.

As a result of this incident and subsequent actions taken by the Subcommittee, there is greater awareness in VA regarding the issue of information security. However, VA still lacks effective internal controls and accountability.

Since July 2006, the VA Security Operations Center has received reports of approximately 3,600 incidents. The incidents included unauthorized access, missing, stolen, or lost laptop computers, improper disposal, and numerous incidents involving unencrypted e-mail messages containing sensitive information.

Of the 3,600 incidents, 250 were referred to the Office of Inspector General. Of these, we opened 46 investigations. One of the most significant is our current investigation of the data loss at Birmingham, Alabama.

Information security remains a major challenge for VA. For example, VA has not yet determined how many employees and contractors use non-VA computers to access VA systems. VA does not know what VA data is being stored on these computers, external hard drives, and other portable devices.

VA also has no means to monitor whether access to data is limited to the information needed to conduct business. And much of VA's databases and e-mail remains unencrypted.

VA will not be able to safeguard data unless three important actions are taken: Hold individuals accountable for compliance with policies and procedures; provide employees with VA-owned computers and encryption software; continue to enhance employee awareness of the need for a cultural change.

Equally important, VA must find a way to implement these actions without impacting VA's ability to fulfill its mission.

Thank you again for this opportunity to update you on the status of our ongoing work. We will be happy to answer any questions you may have.

Mr. MITCHELL. Thank you very much.

[The statement of Maureen Regan appears on pg. 60.]

Mr. MITCHELL. I have a question for Mr. Claudio. You essentially are able to provide a fresh new perspective with regard to field-level activities in information security management at the VA. We welcome your perspective.

Do you believe that policy guidance to the field is comprehensive and unambiguous with regard to information security management and do you believe that the policy guidance is rigorously enforced by field-level managers?

STATEMENT OF ARNALDO CLAUDIO

Mr. CLAUDIO. First of all, sir, thank you very much. And before I start, I want to say that I am honored and privileged to be here today and to you, Mr. Chairman and Members of the Subcommittee, I appreciate the opportunity to come in here and speak truthfully of what I have seen out in the field to you.

Actually, I am very pleased to hear that Mr. Rodriguez and Mrs. Brown-Waite have basically talked about accountability and have talked about putting the point into who is the person to be looked at when we are talking about breaches of data, so forth and so on.

My office was created and actually executed on the 22nd of January. It is an office that is called the Oversight and Compliance. And I do not know. It was not discussed that much over here, but I am the person with my organization to go out there and do assessments on policies, assessments on validation of laws, assessments and safeguard and maintaining in the areas of cyber security, the areas of record management, and privacy.

Within the last 30 days, and by 15 March, we will have completed 16 assessments.

To answer specifically your question, I think the IG basically brought up some very important points in terms of lack of accountability, enhancement of awareness in part. I have gone out and I have reviewed 6504. I have looked at every policy there is. And if you are a person that belongs to VA and you have an understanding of what you are reading in pure English, it is very easy to follow instructions because they are very clear. There are memos to the memos to the memo. There is policy to the policy to the policy and it is all written there.

What there is a lack of, and I think it was brought in, is looking at a person and holding that person accountable for his or her action of what has occurred. And that is really lacking out there. So to be pointed on this is the personal accountability is lacking, number one. So the policy is there.

What it is, and we talked about change of mindset, is change of environment. I have sat in groups where there are 20 to 30 doctors and these doctors, we talked about and discussed how to safeguard the I, which is the information. Still, some of them, even with their high level of understanding of other things, will probably fight the fact that the information is probably not as important as their research.

So what we are looking at is a change of mentality here, which is going to take effect as we go through, and I think the wake-up call obviously on the 6 May and then on the Birmingham piece will definitely change attitudes.

Mr. MITCHELL. Thank you.

I have one other question.

Mr. CLAUDIO. Yes, sir.

Mr. MITCHELL. Do you believe all incidents are reported and do you believe that there are unauthorized reproduction of databases and what is the threat associated with a hypothetical action like this?

Mr. CLAUDIO. Sir, I have been a cop for over 30 years.

Mr. MITCHELL. You have been what?

Mr. CLAUDIO. A cop, a policeman. My last job, I was the Chief of Staff for the Joint Force Headquarters, National Capitol Region, also the senior Military Police in the military district of Washington. And prior to that, I was in Iraq. I was the senior Military Police as an advisor to General Casey.

I will tell you that you have to make some determinations of what you are going to report. There are cases that are insignificant. Your data breaches where they are insignificant of one or two person, that can be handled right there and then and remediation can be taken care of.

So to tell you that every incident is reported, I do not think so. I think with the change of mindset that is occurring right now, you will see the volume of SOC reports actually increasing, doubling, and even tripling because a lot of people are putting conscience into what is going on. So in that term, you are going to see an increase of SOC reports coming into the fact. So that is the first part.

Can you repeat the second part of the question, sir?

Mr. MITCHELL. Yes, sir. Do you believe that there was unauthorized reproduction of the databases and what would be the threat associated with this type of action?

Mr. CLAUDIO. Sir, there is not so much a reproduction. There is a possibility, based on the assessment that I have done, that data is being passed on through unencrypted computers. And because that is done right now, it definitely creates a tremendous risk for the veterans. Yes, sir.

Mr. MITCHELL. Thank you.

Ms. Brown-Waite.

Ms. BROWN-WAITE. I thank the Chairman.

I have a question for Mr. Wilshusen. I am not picking on the VA, but they happen to be our Committee's jurisdiction. If you could tell me of the 150 some recommendations that have been made, what would you say are the top five? And if you—I will let you answer that.

Mr. WILSHUSEN. Okay. First I would like to clarify a couple of things regarding the 150 recommendations. We made these recommendations back in 1998 to 2002. Many of our reviews and our recommendations are very specific, detailed configuration items on computer systems that identify specific computer control vulnerabilities.

VA has to a large extent corrected many of them. However, what they have not done is that they have not taken the next step and proactively looked at the vulnerabilities that we identified on those systems because typically they would just correct the action on a particular system or device that we identified the vulnerability. They did not take the next step to look for and identify other devices or systems that are similar that could have the same vulnerabilities. And we would find those vulnerabilities on similar devices at other locations. So I would just like to clarify that.

But I would say the key recommendation that they still need to address is implementing a robust, centralized information security program. They are starting to make progress in terms of centralizing some of the information security functions and personnel within the CIO's office, but they have not yet implemented all of the key activities associated with a comprehensive information se-

curity program in terms of being able to adequately assess their risk of the impact that could result from an unauthorized security breach to developing the policies and procedures that effectively mitigate those risks, including those configuration, management, and requirements for specific systems and operating platforms.

They also need to assure that their staffs and their security personnel are adequately trained in security requirements as well as security awareness so they know what the threats are and their responsibilities are for implementing the policies and procedures for testing and assessing the effectiveness of controls on their systems and protecting the information on a regular and ongoing basis.

And once they have done those tests, they need to develop remedial action plans to correct and mitigate known weaknesses not just on those devices where they have been identified but across the entire Department.

Ms. BROWN-WAITE. Are other organizations as resistant to change and do other agencies have as much of a problem with breach of sensitive personal information as the VA does?

Mr. WILSHUSEN. Well, I will say that certainly the security breaches at VA have been remarkable and, in fact, stunning in their scope and magnitude. However, they are by no means unique in the Federal Government. Other Federal agencies have suffered and have been exposed to security breaches and data breaches as well.

In fact, one of the reviews that we have ongoing right now is to look at some of the lessons learned regarding similar data breaches at other Federal agencies, particularly as they relate to notification to government officials and effective individuals when such breaches occur. But certainly VA is not unique in the sense that other agencies also have security and data breaches.

With regard to how robust their security controls are and program as compared to other agencies, I would say that they probably are near the bottom of the 24 "CFO Act" agencies. And this is based upon a couple of facts.

One is on the FISMA report analysis, our analysis of their reports have consistently shown that in terms of at least meeting the performance measures that they are required to report under by OMB is that they generally have not fared as well as other agencies.

In addition, the IG and its contractors have consistently reported that they have a material weakness in their information system controls as part of the financial statement audit and in the agency's performance and accountability report, which is another indication that their controls are lacking.

Mr. MITCHELL. Thank you.

Mr. Bachus.

Mr. BACHUS. Thank you.

I will direct this question, I guess, to Ms. Regan. The VA has failed its annual "Federal Information Security Act" review for 6 years in a row, is that right?

Ms. REGAN. I would have Mr. Sardegna answer that question. He is much more familiar with the audits.

Mr. SARDEGNA. I believe we have been doing this since 2001. And, yes, as far as I understand, the VA has never been in compliance with the "Federal Information Security Management Act."

Mr. BACHUS. What happens when you fail that? Are there remedial measures or——

Mr. SARDEGNA. Our past reports have identified 17 different issue areas that we have been reporting for a number of years now. Our reports go to the Office of Management and Budget, and as required we provide OIG information to be included in a joint report with the Department that we send forward.

We also do a separate independent assessment which we provide to what now would be the Assistant Secretary for Information and Technology at the CIO and the different Administration heads of the agency.

Mr. BACHUS. Okay. But, you know, I think everybody, both panels agreed that the VA is not doing, you know, what they should do at the headquarters level at least.

And, Ms. Regan, you mentioned three things they ought to do, is that right?

Ms. REGAN. Yes.

Mr. BACHUS. One was encrypting data?

Ms. REGAN. Yes.

Mr. BACHUS. Is the technology there to have encrypted the data on the hard drive in Birmingham?

Ms. REGAN. You can encrypt the data that you store on the hard drive. There is software that allows you to encrypt the data when you transfer it or work with it on the hard drive. It encrypts the hard drive in itself. The data that you put on there is encrypted through the software.

Mr. BACHUS. Is that made available to the employees in the VA who are downloading this information?

Ms. REGAN. It has not been made available yet to my knowledge. That is one of the issues with our second point. VA needs to provide VA-owned computers so that you can control what security measures are on the computer and buy this encryption software.

Mr. BACHUS. Now, that seems pretty simple really, does it not? I mean, the technology is there. It is not provided. And if it were, it would in this case and many others have resulted in the information that was lost not being subject to misuse or criminal intent.

Mr. SARDEGNA. Well, if I may, Congressman, there are some complicating factors with the Department's IT infrastructure. As the Deputy Secretary has testified, there are multiple platforms. There are many really aging information systems and technologies that VA is trying to bring up to date by adding these new technologies for encryption.

Ms. REGAN. I also believe one of the main issues with respect to this is the cost. We have——

Mr. BACHUS. Is what?

Ms. REGAN. The cost.

Mr. BACHUS. Cost.

Ms. REGAN. I mean, there is a price tag to providing the VA computers, particularly with the emphasis on telework. If you want people to work at home or you have people working at home, VA

would have to buy them VA laptops and have the software installed on them.

Mr. BACHUS. Of course, every time they work at home or every time they have a hard drive, there is a case where somebody could steal that hard drive or they could lose it. I mean, that is going to happen every time, right?

Ms. REGAN. Whatever it is, whether it is a laptop or even a desktop at home or whether it is a hard drive or other portable media device, they can get lost. They can get stolen. It is happening all over the country. I think it gives some sense of security when the hardware or the data was either encrypted or password protected which makes it difficult for somebody to access that data.

Mr. BACHUS. Yeah. And that had not been done to date, right?

Ms. REGAN. That has not been done. Some VA entities have implemented encryption for e-mails but most of VA has not.

Mr. BACHUS. Okay. Let me just close by saying Congressman Mitchell asked, you know, in how many cases is it not reported. And, Mr. Claudio, you said you were a law enforcement officer.

Mr. CLAUDIO. Yes, sir, I was.

Mr. BACHUS. I used to be Assistant State's Attorney General. I can tell you this employee, I do not know him, I do not know anything other than what I read in the newspaper, he reported it. That leads me to believe that is inconsistent with selling it or an intentional act. I mean, and I would say that probably by reporting it, he probably is in the minority of my experience with human beings. In most cases, they do not report it.

Mr. CLAUDIO. Actually, sir, we have seen a change in conduct on that. Like I said before, the SOC report is growing by the minute. There is a conscience out there and a great effort made by the leadership to pass on the message how serious this whole thing is.

And, again, just by going around and assessing what is going on, I think there is being some very heart-to-heart talk from the leadership. As I go around, I meet first with the hospital director and I spend 15 to 20 minutes trying to assess where he or she is in terms of policies, in terms of regulations.

But you can see a definite shift. We are not there yet. It is going to take some time. I think the reorganization is going to pay its fruit. We just got to give some time for that to happen.

Mr. BACHUS. Now, in this case, you had a director of the hospital who immediately notified headquarters——

Mr. CLAUDIO. Yes, sir.

Mr. BACHUS [continuing]. Knowing about the publicity, the consequences. He did his job. I worry about probably for every one of those directors one that says look for it some more, are you sure, you know, or an employee who does not come and report it.

Mr. CLAUDIO. Yeah.

Mr. BACHUS. And I think the answer to that is encryption and policies on, you know, certain information should not be shared with people. You know, I think that probably too many employees have too much information that they do not need to do their job, number one.

Number two, I think this idea of taking stuff home and working on it on your computer ought to have some severe limitations be-

cause, you know, things happen on the way to and from work or at home.

And, number three, encryption technology, a big cost, but, you know, we are going to be here having hearings once a month if you do not have it.

Mr. CLAUDIO. Sir, I could not agree with you more. I think the ultimate thing is that all data from the veterans is collected, distributed within the confinements of that facility period. And then there is enough space inside that server that can handle that so you do not have to go to an external drive, that you do not have to go and plug in a USB port and so forth.

Mr. BACHUS. Or put it on a thumb device or put it on a hard drive and take it home.

Mr. CLAUDIO. Correct, sir.

Mr. MITCHELL. Thank you.

I have just a couple very quick questions for Mr. Wilshusen. First, do you believe that the VA is on the road to achieving the gold standard in information security management?

Mr. WILSHUSEN. If they are, they are at the early stages of that. Certainly since the May 3rd data theft, there appears to have been a change in attitude, at least at the very top.

Secretary Nicholson has testified as well as, of course, now Mr. Mansfield, that it is important that the agency set the tone at the top in terms of what will be tolerated, what will not. And it seems at present at least that they are making that effort.

However, attendant with that is the requirement that you adequately and unambiguously communicate what the expectations are for the employees throughout the entire organization at all levels on what their security requirements are and have that tied then to their performance standards, their position descriptions, communicate that through various forms of directives, handbooks as the VA is attempting to do.

And then once you have communicated what those expectations are and provided training to the staff is to make sure then that there are accountability measures in place that reward those that do perform and address those that do not.

Mr. MITCHELL. Earlier, Mr. Claudio said there were memos on memos. There was every written rule in the world. I mean, that is not the problem. So I do not know how these employees could not know what is expected of them unless their supervisors are not doing their job.

Mr. WILSHUSEN. Well, that is exactly right. You need to have the enforcement and accountability mechanisms in place, be that through performance mechanisms, through their ratings, and where it affects them in either the paycheck or have other administrative actions.

The other thing that you have to do because people are only one part of the overall equation related to information security effectiveness in an organization, you also have process and technologies. Often people will be your weak link in many cases, but you need to have controls and other disciplines through the technology, make sure you have appropriate technology controls to include things like encryption, to include strong access controls on your systems.

You also need to have appropriate processes and part of that is making sure that those individuals only have access to the information that they need to perform their job and that they control that information and do not allow it on laptops or removable media when it is not needed to perform their job.

And if it is, to make sure you have the appropriate technical controls to help protect that information when it is at risk because the information can be at risk at multiple places, both at rest when it is on the hard drive, when it is on a server, or when it is being transmitted across a network or over the Internet.

So there needs to be appropriate controls and policies in place. And by policies, I mean technical security control policies in place to protect that information.

Mr. MITCHELL. And a couple other quick questions. How does the VA compare with other agencies with regard to information security management programs?

Mr. WILSHUSEN. Well, I would say that, you know, based upon the reporting mechanisms afforded by FISMA, the "Federal Information Security Management Act," and based upon the results of audits and reviews of information system controls performed during financial statement audits that VA is probably near the bottom.

Just to illustrate, VA has had, I guess, a material weakness in their performance and accountability report and information system controls since 1997 each year.

In addition, for 4 of the last 5 years, the House Committee on Government Reform has been issuing computer security report cards based upon an analysis of the annual FISMA reports. And VA has received a failing grade for 4 of the last 5 years.

And as I mentioned earlier, VA has not yet submitted its official draft or its official copy of its annual report this year.

Mr. MITCHELL. Can you tell us of the successful agencies best practice?

Mr. WILSHUSEN. In terms of agencies which have done that?

Mr. MITCHELL. Right.

Mr. WILSHUSEN. Well, by those same standards and criteria that I just laid out, some would include perhaps like Social Security Administration. They have not had a material weakness or reportable condition on their financial statement audits. They have consistently scored higher on the review of the FISMA reports.

A couple other ones would include, I think, National Science Foundation. But I would also caution that though they have done well on the FISMA reports and also as part of the financial statement audits, because those reports and audits are somewhat limited in scope does not necessarily mean that they have full and highly secure systems.

Mr. MITCHELL. Ms. Brown-Waite.

Ms. BROWN-WAITE. Thank you.

Earlier during the previous panel, my colleagues, Mr. Davis and Mr. Stearns, had suggested an outside audit and investigation group come into the VA.

And I do not know who can answer this. If they are ignoring the IG and the GAO, why would an outside group perform any magic and results that are not exactly being accomplished here with your report and the followups?

Mr. WILSHUSEN. Well, one, first of all, I think it is always appropriate to have independent reviews of an information security program or the information security controls in place at an agency are all on particular systems. Indeed, that is what GAO and the IG have done on many reviews in the past.

The basic problem is they have not implemented an appropriate information security program. And it will take probably a sea change for them in order to do that. You know, certainly an independent review from an outside source could provide other skills perhaps, but at the same time, I think the reviews that the IG and we have performed highlighted significant vulnerabilities and gaps in security controls.

Ms. BROWN-WAITE. If I may ask a followup question. Would it be better for Congress to say—I know this is a terrible word to use—to earmark, to make sure that money is set aside specifically for the kind of security, data security that we need with no ifs, ands, or buts about it, take money from their existing budget and say, "you will do this?"

Ms. REGAN. I was going to say I think it would depend on what you are going to ask them to do with the money. If it is going to be this money will be set aside for encryption and laptops, that is one thing. I think what needs to be done first is to have the resources put to those needs. So I think you would have to identify what aspects and how much money to begin with.

One other issue, if I could follow up on the contractor issue, I think as we noted in our report last summer, the July report, VA still has serious problems with contractors and access to our data. If you remember, the UNISYS computer got stolen that had VA data on it.

I think, though, the Department is making head way to do this. I would be concerned that the scope of any contract would have to be defined, and I am not sure how long it would take to define the requirements. VA does not have a good history with IT contracts. And I think it would have to be defined, but I am not sure it would be done in the very near future. I think you may be looking down the road for a while, unless it was a narrow scope contract on one issue.

Ms. BROWN-WAITE. I think Mr. Claudio——

Mr. CLAUDIO. Yes, ma'am. I think it is a matter of capability. If you look in the past, the question is, did we have the capability to do such an assessment. We did not. Thirty days ago, that organization was put together. It is the organization of Oversight and Compliance.

Basically it is an organization that covers the entire United States, including Alaska, Hawaii, Puerto Rico, Guam, and the Philippines. It will do about 16 to 20 assessments per month once the full capable organization. So we probably will have to ask that that capability to get function and go ahead to see how productive that is.

We have met with the IG, the organization. We have discussed this point. And if you look at, there is about 266 medical centers. There is about 63 regional centers. It is about 300 plus. All those regional centers and medical centers will be assessed about in a

year and a half. So the assessment capability is now there and we just got to give it some time to see where we get from here to there.

Mr. MITCHELL. Thank you.

Mr. Bachus.

Mr. BACHUS. Yeah. I would like to just ask two followup questions. My first one is about the Birmingham breach, but it is not directed at Birmingham because I would bet you this information went out to a bunch of other sites too.

But why would anyone in the VA, in VA research or VA in general, need access to the entire CMS database on everyone that ever billed CMS for healthcare, including all that information, or if they were, you know, why could that not have been encrypted or why could it not have been under some very tight supervision?

Ms. REGAN. That issue is actually being addressed in our administrative investigation. We are looking at this point as to why that individual had that data. We are also looking at why the individual was given all the fields that are in that data set and whether they were necessary. We are also looking at whether or not CMS should have given that database to the VA to start with, there are key factors of the database that VA was never given or that were not given to the facility. But why that information on that many physicians? Was it necessary at various levels? It did not go to this individual initially. It went to somebody else who he works with. But we are looking at all of those various issues regarding that database.

Mr. BACHUS. Okay. Thank you.

Has the VA inventoried or restricted employee access to sensitive veterans' personal information on a need-to-know basis?

Ms. REGAN. The VA has not inventoried it as far as I know. But I do know that when you access a database, you need to explain and get it approved to have access to the database and usually what part of the database and for how long, and whether you are just going to review it, if you are going to copy it, there are various questions that are asked.

It gets down to the individual level. Is the individual ISO, information security officer, or the CIO who has responsibility at a facility asking the right questions? Is it for a limited time period? Do you need all the fields in the database? All those issues should be addressed. So it gets down to an individual level, but there are measures in VA to do that. It is whether or not people comply with it.

Mr. BACHUS. All right. Thank you.

Mr. MITCHELL. Thank you.

One quick followup. Mr. Wilshusen, you mentioned some paperwork that the Veterans' Administration has not completed for information security. Could you repeat what that is again?

Mr. WILSHUSEN. Yes. The "Federal Information Security Management Act" requires agencies to report annually on their progress in implementing the provisions of the Act. They are required to report in accordance with OMB's instructions on reporting for this. OMB has set up a number of performance measures and a reporting format for that and requires the agencies to report by October 1. It is called the Annual FISMA Report.

As of today, VA has not submitted its official copy of that report. Now, it has submitted a draft of that report to OMB, but has not yet submitted the official copy. And accordingly, because it is a draft, both GAO and Congress are also supposed to receive copies of these reports and we have not received them yet.

Mr. MITCHELL. Have you heard anything from the VA about why they have not done it?

Mr. WILSHUSEN. I do not know precisely the reason why. As far as I know, perhaps—well, my colleagues might know why.

Mr. MITCHELL. Does anybody know? I understand. Assistant Secretary Howard, would you address that question?

Mr. HOWARD. Sir?

Mr. MITCHELL. Why the paperwork has not been submitted.

Mr. HOWARD. If it is the same report I am thinking about, it is in the Secretary's Office with signatures.

Mr. MITCHELL. And this is February, right, and it was due in October? I mean, this is March really.

Mr. HOWARD. Yes.

Mr. MITCHELL. Thank you.

Mr. BACHUS. Could I ask one followup question?

Mr. MITCHELL. Yes.

Mr. BACHUS. I do not know if it was this panel or the last panel said that in the aftermath of that May 3, 2006, the massive breach there, that the VA issued a directive that you could not download sensitive personal information about veterans, maybe physician providers too—I do not know—onto—it had to be a VA computer—I do now know exactly—or VA-owned equipment, I think.

But that has been now waived, is that right?

Ms. REGAN. There was a subsequent memorandum that waived that provision for the three Administrations, which would be National Cemetery Administration, Veterans Health Administration, and Veterans Benefit Administration.

Mr. BACHUS. So which is about all of VA basically, right?

Ms. REGAN. Pretty much. It would not only just be the databases. It would just impact the people using those databases within those Administrations. People in OIG offices may have access to those databases for oversight purposes. It would not affect us. We have our own policy that only VA-owned computers can be used, not personal computers.

Mr. BACHUS. Was that just as a practical matter? Once they did that, they prohibited that, that the system just could not work?

Ms. REGAN. I do not have any knowledge as to why it was done. We have never seen the justification.

Mr. BACHUS. I mean, why it was waived.

Ms. REGAN. Why it was waived. The reason they put the policy in place——

Mr. BACHUS. The prohibition.

Ms. REGAN. Right.

Mr. BACHUS. I can understand the prohibition. I do not understand why it was waived unless maybe as a practical matter, they could not pay benefits, they could not treat because, you know, maybe it interfered with their—but it would be interesting to know.

Does any of the panel know why a temporary waiver was issued? Thank you.

Mr. MITCHELL. Any other questions?

Thank you very much. I appreciate it.

Ms. REGAN. Thank you.

Mr. MITCHELL. And at this time, we are going to have the third panel, and this should go—they do not have opening statements. And I would like to, while they are getting ready, read a statement.

The Minority Members had requested these witnesses for this panel so that we could gain better insight into information security management and research-related programs at VA.

Ms. Regan, could you just hang around a little longer because I think I would like you to sit in on this if you would.

This was an act of choice and I fully concur with the request. I do regret that we could not provide VA with more time to coordinate the appearance of one REAP Director, Dr. Pogach. I appreciate you responding in short notice.

I would also like Ms. Regan, Counsel to the VA Inspector General, to sit in with panel three to advise us if in her opinion the questions or answers get too close to the nexus of the IG's ongoing investigation so as to jeopardize that investigation.

I also welcome from the Birmingham VA MC, Mr. Parris and Dr. Blackburn.

TESTIMONY OF LEONARD M. POGACH, M.D., DIRECTOR, RESEARCH AND ENHANCEMENT AWARD PROGRAM, VA NEW JERSEY HEALTH CARE SYSTEM, EAST ORANGE, NEW JERSEY; WARREN BLACKBURN, M.D., ACOS/R&D COORDINATOR, VA MEDICAL CENTER, BIRMINGHAM, ALABAMA; AND Y.C. PARRIS, FACILITY DIRECTOR, VA MEDICAL CENTER, BIRMINGHAM, ALABAMA

And we are just going to open this up to questions.

And, Dr. Pogach, did I pronounce your name right?

Dr. POGACH. Yes, sir.

Mr. MITCHELL. Okay. Well, thank you for being here today. I appreciate it. And could you please explain what the REAP or REAP Program is and why researchers in that program require the use of large databases?

Dr. POGACH. It is a Research and Enhancement Award Program. These are competitive center awards, mid-level center awards which are awarded by the VA Health Services Research and Development Program. I am not sure how long the program has been in existence. We were awarded, our center in New Jersey, in September 2003.

The purpose of the center is each of them has a theme. We are interested in healthcare knowledge management which includes chronic illnesses and quality management. The REAPs are awarded to those facilities that have demonstrated certain research capacity and capability.

And one of our specific interests, not the only one, is the use of large databases to basically look at the quality of care provided to veterans as well as their course over time in terms of looking at whether or not the quality of care provided results in improved out-

comes, such as decreased morbidity, decreased mortality, for what I do especially with diabetes.

The reason why large data sets are required is these types of outcomes, which are observational, often are not able to be attained through clinical research. For example, clinical randomized trials, especially when you are looking at the variation in outcomes among a wide variety of facilities across a national system.

And this sort of data and analyses and publications certainly can result in not only publishable research, but the goal would be to provide information within the VA on where there is variation in care, variation in outcomes that might allow managers to be able to track where to look for interventions.

And second of all, what we would really like to do with our quality improvement program, which most of you probably are aware of, the VA is a leader, is to actually determine if we can go beyond provision of—we did process. We lowered a value to something to really see if veterans are living longer and living healthier.

Mr. MITCHELL. One other question. Do you share any researchers with other non-VA organizations and, if you do, how would you assure with reasonable certainty that information security practices are being followed?

Dr. POGACH. We do not share the data that we get for all large database analyses with other organizations.

Mr. MITCHELL. But do you share the researchers?

Dr. POGACH. Do we share the researchers?

Mr. MITCHELL. Yeah.

Dr. POGACH. We have WOCs who are shared with other universities, yes, but when they work with us they are working on-site and on VA grounds. The salaries may be shared.

Mr. MITCHELL. And you are fairly certain that the information security practices are being followed?

Dr. POGACH. Yes. The security practices now that we have are very clear as to what we do. In part, we are also a relatively young REAP in terms of how we have been funded, and we did not have strong preexisting relationships with our organization.

So we developed our program to be in-house. I understand that is not the case routinely across the entire VA system, but our capacities and our data systems are within our VA.

Mr. MITCHELL. Thank you.

Ms. Brown-Waite.

Ms. BROWN-WAITE. I thank the Chairman.

Dr. Weeks, could you tell us why the REAP research was suspended at your facility?

Dr. BLACKBURN. I think you mean me, Dr. Blackburn.

Ms. BROWN-WAITE. Oh, okay.

Dr. BLACKBURN. Yes. The Office of Research Oversight after finding out that the external hard drive had gone missing suspended the REAP research activities.

Ms. BROWN-WAITE. I mean, will they resume?

Dr. BLACKBURN. That is certainly our expectation and hope. To my understanding, the ORO's investigation is ongoing and has not been completed.

Ms. BROWN-WAITE. And, Dr. Blackburn, as long as I have you there, do you know why this happened on your watch?

Dr. BLACKBURN. The investigator or the programmer had an external hard drive within VA space. From what I have been told by him, it was stolen.

Ms. BROWN-WAITE. Well, why was it not encrypted? I think that is part of the problem.

Dr. BLACKBURN. Well, I think as panel two——

Ms. BROWN-WAITE. That is the problem.

Dr. BLACKBURN [continuing]. Already VA has not provided at this point encryption software for external hard drives. We have gone ahead in Birmingham and taken additional actions that we have now banned external hard drives, and our VISN is in the process of banning all but a few thumb drives.

Ms. BROWN-WAITE. And the repercussions if you violate the ban?

Dr. BLACKBURN. I am sorry. I did not hear that question.

Ms. BROWN-WAITE. The repercussions if the ban is violated.

Dr. BLACKBURN. Well, I think the thing is we are responsible and we are aware of who buys hard drives. So we know where they are and we have gone ahead and collected them. The thumb drives are going to be, to my understanding, inoperable based upon a computer patch except the ones that are——

Ms. BROWN-WAITE. I want to make sure I understand what you are saying. Someone cannot go out and buy one at Office Depot and download onto it?

Dr. BLACKBURN. That is my understanding of the plan of the IT folks within our VISN, correct.

Ms. BROWN-WAITE. That is your understanding of the plan. Is that what the plan does?

Dr. BLACKBURN. Is that what what?

Ms. BROWN-WAITE. Is that what it actually does is it prohibits downloading on a thumb drive?

Dr. BLACKBURN. Unless it is an encrypted thumb drive, that is correct.

Ms. BROWN-WAITE. And for all three panel members and Ms. Regan, if you can contribute, I certainly would welcome that. The question is, you know, what did you individually do to implement the VA directives 6500 and 6504 on cyber security directly after last year's May 3rd incident?

Mr. PARRIS. We strictly enforced that directive. We made sure that any external device was within that work space. The one area actually that was involved with this actually went above and beyond.

They actually met with our staff on just a security, if you will, education program and they made their own policy that when the person who was using a drive was not in the vicinity of that drive, which is totally legal for it to be by the policy, that they actually lock that up in an additional locked area. So they went even beyond the policy within that particular area.

Ms. BROWN-WAITE. Whenever I check into a hotel or motel when I am traveling and there is that big sign up there that says no swimming after ten o'clock, I always say to the owners what is the penalty if I go swimming after ten o'clock.

So I want to know what you all do to actually implement and enforce this, because I am getting the impression that we have so many written policies out there, policy upon policy and directive

upon directive that maybe that is part of the problem, that the employees may be totally confused when they have a directive de jure.

But what is being done to implement and enforce the prohibitions where they do not swim after ten o'clock?

Mr. PARRIS. We have gone through extensive education with our staff. We have gone as far as having an information security fair for a better term. We invited people up to a full day so that they could get trained on what we meant by information security.

We have on our Web site all the policies. We have a question form for those policies for the ones who may not understand some of the questions.

I do not know if I am answering your question with the look on your face, but, you know, I am trying to get to the gist of the question.

Dr. BLACKBURN. Well, let me go ahead and add that we have required, as Mr. Parris indicated, training for every one of our employees who have access and it is real simple. If they did not go through the training, their access was cut off.

Ms. BROWN-WAITE. So was this after the latest incident that happened at——

Dr. BLACKBURN. No, ma'am.

Ms. BROWN-WAITE [continuing]. Birmingham?

Dr. BLACKBURN. No.

Ms. BROWN-WAITE. So it was before?

Dr. BLACKBURN. That is correct.

Mr. BACHUS. Let me start by saying that I know Y.C. Parris. He is a great Director and operates a very good ship. So I ask these questions. I do not need to apologize to ask them, but I have an obligation to ask it.

And what I kind of heard earlier was that you all complied with all the procedures and the directives from VA, is that correct?

Mr. PARRIS. Yes, sir.

Mr. BACHUS. But now, am I confused or were the directives, did they not include that you all encrypt this information and that that was not done?

Mr. PARRIS. No, sir. That is part of maybe what the Congresswoman was getting at, that there was a little bit of ambiguity. And if you look at the policy, it says within the external hard drive, which we do not have the software available to encrypt the external hard drive at this time, that if that hard drive is within that secured work space, that office space, whatever it is that is VA property, then that is okay.

Mr. BACHUS. It does not have to be encrypted?

Mr. PARRIS. No, sir.

Mr. BACHUS. But I guess they say either keep it in a secure location or encrypt it?

Mr. PARRIS. Yes, sir.

Mr. BACHUS. But then you do not have the software nor did they supply the software to encrypt it?

Mr. PARRIS. That is correct, sir.

Mr. BACHUS. Which is almost a directive without the ability to comply, is it not?

Mr. PARRIS. It makes it very difficult, yes, sir.

Mr. BACHUS. I mean, I guess you could go out at your own expense, and I do not know. But, you know, it would seem that if they would supply you with information, require you to encrypt it, they would provide the software and the means to do that as part of the system. That would have been an easy way to avoid what happened in February, I would think.

Mr. PARRIS. Yeah. The horse and the cart.

Mr. BACHUS. What?

Mr. PARRIS. The horse and the cart. And Bill Gates just had an article in the paper recently that illustrated that where he said that when you see how fast technology has moved, that our security system is like a stone castle with a moat around it and a drawbridge, but the technology is a jet plane with missiles on it.

Mr. BACHUS. Now, the IG reported that, you know, it would be good to encrypt this information. And I am hearing in this hearing that software is available to encrypt the information, but the VA up here, I will tell you, they are going to want to shift part of the blame and said you all should have encrypted it. We sent a directive to you to encrypt it, but you were not given the software. But you were also told that it could be within a secure area. And you are telling me it was within the work space.

Mr. PARRIS. Yes, sir.

Mr. BACHUS. And the employee, when he discovered that it had been taken or that it was no longer there, he reported it promptly?

Mr. PARRIS. Reported to my office, yes, sir.

Mr. BACHUS. And you reported it promptly to D.C.?

Mr. PARRIS. Reported it to my network director, which is my protocol, who was in Atlanta, and he reported to D.C. the same timeframe.

Mr. BACHUS. Now, they have suspended your research and that of also six other centers which as they inquired, they discovered that they had not encrypted information, including, I guess, the White River Junction facility, is that right?

Dr. POGACH. Actually, from New Jersey, but they suspended all the REAP programs.

Mr. BACHUS. I cannot hear.

Dr. POGACH. I am sorry. We are from New Jersey. I am not from White River. Dr. Weeks could not make it today. But all the REAP programs——

Mr. BACHUS. Are you from East Orange or where?

Dr. POGACH. Yes, New Jersey.

Mr. BACHUS. Okay.

Dr. POGACH. So all the REAP programs were suspended not specifically for any one issue but to allow for reassessment of all data security at those sites.

Mr. BACHUS. But was one reason it was suspended because the information was not encrypted?

Dr. POGACH. I do not know the reasons why, if that could have been one reason or not. We were just basically told that all research is suspended so that we could basically make sure all policies——

Mr. PARRIS. No, sir. I think it was due diligence on the part of the organization.

Mr. BACHUS. I am not arguing with their decision to shut down the programs and assess whether that information should be out there in the first place and, if it is, it ought to be encrypted because people are going into places and steal things.

Dr. POGACH. Right.

Mr. BACHUS. Thank you.

Mr. MITCHELL. Mr. Walz.

Mr. WALZ. Thank you, Mr. Chairman, and thank you, gentlemen, for joining us.

I am sorry I missed your earlier testimony, Mr. Parris, when you—your initial statements on this. I was here earlier for Deputy Secretary Mansfield, and I am looking at some of the things he said.

We had a long discussion in that first panel on the idea of what role culture plays, culture in an institution, as you are well aware of. And I am listening to my colleague, Mr. Bachus, talk about it. And I have no doubt. I am a veteran and I understand and I have the greatest respect for the VA and the work that you do. Absolutely critical.

And as I stated in that first panel, the intentions, I am always operating from the assumption that the best intentions are always what is there.

When looking at these data losses, I am just trying to get my mind around it as a veteran, as one of those people who got one of those letters, what can we do to prevent it, what can we do to stop it.

And when I am looking at this and I think about my job, my former job as a high school teacher in public schools, data privacy is the air that we breathe. And we have got a lot of people in public schools, namely our students, who are pretty darn good with computers. And, yet, it is just stress to us.

And there are password changes every 21 days. There is log-out timeouts and log-out restrictions. If your computer is shown as being idle and logged in, you get notified and you get called in and written letters on those types of things because they are really critical. There are student data that could get into health issues, too, that are on there.

So my question is, and Deputy Secretary Mansfield was very candid and very open about some of the restrictions that were put on him, I understand your job, Mr. Parris, is to provide the highest quality healthcare you can to your patients. That is your number one priority.

This data privacy issue is part of that and might be seen as a peripheral or distraction. We understand how important it is. I am still trying to figure out, in your mind or in your assessment, is this a resource issue or is this a cultural issue inside the VA on the importance of safeguarding this data?

And I am asking you in the broad range because, as I said, I am operating from the assumption you want absolutely the best care for our patients and you want their data secured. I want the same thing. How do we get to that?

Mr. PARRIS. Yes, sir. I agree with you about your last statement about wanting to secure the data and make sure we take care of our patients. I do not want to throw a wrench into this, but I think

it is neither totally culture or resources. Both of those, you always deal with and they are always going to be there.

But I think it is the growing pains. I am probably the only person in the room who has been around since Crew DHCP. That is where we had four contractors and we were testing computers and the only thing we had on there was a patient history. And we have grown to the most sophisticated medical record in the world right now in the VA system.

And the growth of that, within the growth of the patients and the growth of the system we have, and then we have three major entities. Besides VHA, we have VBA, which is a huge entity, and then we have National Cemetery. And the things they do are different.

And so I think it is growing pains as much as anything, is how do you stay up with the change in technology, the new software that is coming out. I do not know how many times I have sat at a table like this and talked about if we only had a patch on that software, we could get the patient what they need quicker. Can anybody write a patch for that?

So you see the complexity of the system that we have. And I think that to have the people in the know to help keep up with the security part of that, as I talked about the castle and the airplane, that is really kind of the gap that we have, and how do we make those come together. How do we have a security system that runs parallel with the technology that we are installing on a daily basis?

Mr. WALZ. I appreciate that. There was a suggestion earlier, and I am just getting your feeling on this because we all want to solve this, whatever it is going to take, and I just see a massive need that the public wants this, because one of the things, as you well know, the biggest thing for me as a veteran that it is the loss of trust, which is critical to us. Of all the good work you do, you hate to see that happen.

And it was suggested by Mr. Rodriguez that we just need to maybe provide a crack team of people that provide the best security or whatever it is from wherever they come from and drop them in here and get this thing done.

Now, do you believe that is the solution or is this part of the growing pains, that that would not do it? They would not understand your organizational needs the way you understand them?

Mr. PARRIS. With all due respect to that suggestion, sir, I do not think that would solve the problem. I think that would be another expenditure that probably could be spent on a solution to the problem internally.

Mr. WALZ. Thank you so much.

Ms. BROWN-WAITE. If the gentleman would yield. I asked that question before because my fear is you bring an outside group in, they are going to ignore those recommendations as they have ignored the IG as well as the GAO. And I would rather see the money spent on some kind of a solution soon here.

Mr. WALZ. Software.

Ms. BROWN-WAITE. Right. Software would be great. But, you know, also setting that what are the consequences of not securing that data. And it is not just in the VA. I think every agency is probably guilty of it.

Mr. MITCHELL. Thank you.

I think that will be all. Just before we adjourn, I would just like to know and I think this Subcommittee would like to know when the Secretary signs the FISMA report. I would like to know that. So if somebody here could let us know when it is actually signed, I would appreciate that.

And if there is nothing else, this meeting is adjourned.

[Whereupon, at 5:30 p.m., the Subcommittee was adjourned.]

A P P E N D I X

Prepared Statement of Hon. Harry E. Mitchell
Chairman, Subcommittee on Oversight and Investigations

I have accelerated our Subcommittee's review of VA information security management for several reasons. I thank all three panels of witnesses and our Subcommittee Members for their cooperation despite the somewhat short notice we were able to provide. It is my belief that when the subject matter justifies some sort of review, that such a review should be thorough, balanced and timely.

This topic was on the Subcommittee agenda for later in this year. While it is a recurring and non-partisan topic for our Veterans Affairs Committee, the events regarding the data loss at Birmingham and other circumstances have led me to advance this hearing on our Subcommittee docket.

In this hearing I wish to determine the current status of information security management at VA. Admittedly, the Birmingham incident holds powerful sway over the landscape. If the Birmingham incident stood alone against a backdrop of a sound information security management program perhaps we could address a one-time-only incident with more patience.

However, the record reflects a host of material weaknesses identified in Consolidated Financial Statement Audits and Federal Information Security Management Act [FISMA] audits over recent years. The Inspector General's Office and the Government Accountability Office have both reviewed VA and found deficiencies in the information security management program over the last 8 years. VA is slow to correct these deficiencies. For example, the VA IG made 16 recommendations with regard to information security management in 2004—all 16 remained open in 2006.

During our full Committee review of the May 3rd, 2006 data loss, we discovered a general attitude regarding information security at VA that our current full Committee Chairman Bob Filner once referred to as a "culture of indifference." Today, I wish to address this issue of "culture" and the need for cultural change with regard to information security at VA.

Last year, the Committee reviewed cultural problems at several levels at VA.

We looked at the very top levels of VA leadership and were critical.

We looked at the program leadership level and were critical.

We looked at the promulgation of information security policy in VA and were critical of the various methods employed by some program leaders and advisors to gut those policies, to avoid accountability and to weaken information security practices.

We were critical of the lack of checks and balances in the information security management system at VA—was guidance being followed, did oversight occur?

We were critical of the delay by VA in providing congressional notice of the May 2006 incident. We were critical of the slow escalation in notice of the magnitude of that problem.

VA mailed notices to millions of veterans addressing the data compromise and made a public commitment to become the "gold standard" in information protection within the Federal Government. Eight months after the initial data loss, VA reports another loss of significant magnitude associated with a Birmingham VA research program.

That a weakness existed in this area surprised no one. That it happened at all serves to precipitate this type of congressional oversight hearing. While the *actual loss* of the external hard drive and the limited electronic protections on that missing equipment should be considered the 800 pound gorilla in this room, there were some silver linings with the Birmingham story as we now know it.

For example, the loss was reported in VA and quickly relayed to the appropriate people. Mr. Howard notified congressional oversight staff and Secretary Nicholson called the Chairmen and Ranking Members of the VA Committees. The Office of the Inspector General was quickly involved and opened an investigation.

In similar examples from May 2006, VA took days or weeks to accomplish those tasks—in the Birmingham incident of January 2007, VA took hours or days to ac-

complish the same tasks. Staff was notified within 1 day, and calls from the Secretary followed a few days afterward. The investigative trail was reasonably fresh for the IG to follow.

What of VA culture with regard to this issue? The IG made five recommendations to the Secretary in their "*Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans*" on July 11, 2006. As of today, all five of those recommendations remain open. Why?

After the 2006 series of hearings, VA issued a series of tough sounding declarations, but problems still remained and another major incident has happened. After the Birmingham incident, the Secretary issued some tough guidance, but what impact will it have? Will history repeat itself? How deep are the cultural barriers?

I believe that it is important to review all aspects of this issue. We need to hear from VA leadership and in that regard we are pleased that Deputy Secretary Mansfield has agreed to testify. He, Secretary Nicholson, the Under Secretaries are key to setting policy—they represent the Department in this matter.

But we also need to look at this problem through the eyes of the remaining 200,000 plus people in the VA. Do leadership actions throughout the management hierarchy match policy guidelines everywhere in VA?

Do the rules say "no" but the culture beckons, "Aw, go ahead—make an extra copy of the data and your life will be easier." "Take a short-cut, no one will follow up." If we change the culture at VA we can begin to fix the problem.

But people have different cultural perspectives; those of the VA leaders on panel one may differ from those of the researchers in the field. Leadership's policy guidance may now be spot on, but the question is how that policy is received at the user-end. For that reason, this Subcommittee requires testimony across the spectrum of people who in any way handle sensitive information about our veterans. Let us approach this with open minds, consider other perspectives, and be able to put this problem to rest for a long time.

Before I recognize the Ranking Republican Member for her remarks, I would ask our Members' consent for a guest and permit Congressman Artur Davis from Alabama to sit at the dais and be allowed to ask questions after all Subcommittee Members have had that opportunity. Without objection?

I now recognize Ms. Brown-Waite for opening remarks.

Prepared Statement of Hon. Ginny Brown-Waite, Ranking Republican Member, Subcommittee on Oversight and Investigations

Thank you, Mr. Chairman.

Our hearing today, as the Chairman indicated, is to learn more about the Information Security Management at the Department of Veterans Affairs, in particular, the current effectiveness of information security at the Department, and the need for cultural change.

Since the data breach of May 2006, the second largest in the nation and the largest in the Federal Government, we have seen the VA's centralization of the VA's information management, including information security. I appreciate the Secretary's desire to make the VA the "Gold Standard" for information technology and information security management in the Federal Government. From what we have seen, adherence to the Federal Information Security Management Act (FISMA) has not been adequately addressed governmentwide, as Congress intended when writing the law. This is why our Committee worked so hard last Congress to pass measures such as H.R. 5835, and the final version of S. 3421, which became Public Law 109–461. We have tried to give the Department, and in particular, the Secretary, the tools he needs to mandate change within the entire Department to make certain that such security breaches are few, if any.

I have served on this Committee for 4 years, and recently been selected as the Ranking Republican Member of this Subcommittee. Over the years, I have seen the lack of resolve within the underlying culture at the Department, particularly at the facility level, to change the way senior management view IT security. It is sometimes difficult to embrace change, and this is what we need to address in this hearing. In order to protect our veterans, and provide them with the services they need, we need to remove that cultural predilection against change.

I appreciate the witnesses who have come to this hearing, particularly those who have traveled a distance to be here, and I look forward to hearing your testimony.

Thank you, Mr. Chairman, and I yield back my time.

Prepared Statement of Hon. Gordon H. Mansfield,
Deputy Secretary, U.S. Department of Veterans Affairs

Thank you, Mr. Chairman. I am here before this Committee on behalf of the Secretary and the Department to discuss with you the changes underway in the Department of Veterans Affairs Information Protection program. The Department has committed itself to becoming the "*gold standard*" in Information Protection within the Federal Government. We have made significant progress in a very short period of time to reach this goal. Nonetheless, we realize that there is much more to do, and we have positioned our Information Protection program to undertake the challenges before us . . . and to succeed.

Early on, the Secretary recognized the need to reorganize our IT assets to give the Department's Chief Information Officer, and Assistant Secretary for Information and Technology, full control over our IT budget, people, and programs.

This Committee was heavily invested in that decision. It held numerous hearings to assist the Department in addressing the many issues involved in centralizing our IT function.

We created the Office of Information Technology and transferred over 4,500 employees to this new organization. These VA employees are under the supervision and direction of VA's CIO, Bob Howard. We are currently completing the final phase of our reorganization by bringing the full complement of IT programs, dollars, and people under Assistant Secretary Howard's control.

This reorganization is a Departmental priority. All leadership elements—from Central Office to field locations from Maine to Manila—have been briefed and instructed. Command emphasis is firmly on information security. And it is squarely focused on revamping our IT infrastructure—from practices and procedures . . . to our Department's data security culture.

We are also committed to creating a dedicated IT career field that will help us to develop, recruit, and retain the bedrock of professional IT careerists we need today if we are to meet the challenges of tomorrow. I personally have spoken to departmental leaders on this critical issue.

To improve the delivery of IT services as we transition to a centralized IT program, we brought in outside consultants, including IBM, to assist in professionalizing our systems. IBM recommended that we change the way we manage and direct IT. We have done that. We have reduced the scope of work and narrowed the span of control of our IT senior leaders. By *telescoping* their management focus, we expect more efficient execution of their responsibilities and, in turn, better results and outcomes.

Significant issues remain in the area of Information Protection. We are addressing them head-on. We have begun to revamp our entire program, consistent with IBM recommendations. Over the past six months, I have spoken with many VA employees, at all levels, to underscore the Department's unqualified position on the IT reorganization. I have stressed the importance moving-out smartly to take charge of the difficult issues at hand. And I believe the vast majority of VA employees are now more aware . . . more sensitive about data management and security in both the *administration . . . and in the delivery of services* to veterans and their families.

Previously, the head of our Office of Cyber and Information Security was assigned such a wide span of control that it was difficult to excel in all areas of responsibility. As a result, support of our Administrations and staff offices suffered.

We have since created a more comprehensive approach by establishing an Office of Information Protection and Risk Management. Its management oversees several key areas. Cyber Security focuses on FISMA reporting and policy development. Risk Management and Incident Response addresses risk assessment, incident resolution and credit monitoring. Records Management and Privacy focuses on policy development and oversight of privacy and records. Data protection analysis and *lessons learned* are also an integral part of this new management focus.

Our field-based Information Security Officers have been operationally realigned to report to the Office of Field Operations and Security.

And finally, we consolidated several IT compliance programs within the Office of Oversight and Compliance, which reports directly to the Assistant Secretary for Information and Technology. This office will conduct rigorous assessments nationwide. Both announced and unannounced, these reviews rigorously evaluate facility compliance with legislative directives as well as policies, procedures, and practices relating to information protection, data management and control, data, records management, privacy, and IT security programs.

This office will be the *first responder* to facilities where serious IT security incidents occur and that require the immediate review of records management, privacy, and cyber security business practices. I am confident that this office will provide the

further assurance necessary to bolster our records management, privacy, and data security measures.

On June 28, 2006, the Secretary delegated to the Assistant Secretary for Information and Technology the responsibility for Departmental Information Security. Since the May 2006 data security breach, VA has issued eight IT directives on specific IT security safeguard requirements. We have developed a comprehensive strategy to incident resolution that includes procedures for notifying veterans of incidents where personal information has been compromised. We have drafted a regulation to implement the Veterans Benefits, Health Care, and Information Technology Act of 2006. And our Oversight and Compliance Office, established this month, has already completed several facility assessments.

We have launched a number of technology initiatives, both completed and underway, to protect sensitive information. We have encrypted over 15,000 VA laptops. We are minimizing the use of thumb drives and mobile devices. Where authorized, we are requiring them to be encrypted. Very importantly, we are in the process of testing technology that will check for proper encryption, codewords, and security credentials necessary to be permitted entry into VA's information network.

The gravity of information security is undeniable. Data security incidents such as we have seen tarnish VA's reputation and the peace of mind of those we serve.

We are aggressively instituting a VA-wide change in culture and mindset across the length and breadth of our facilities, urban and remote.

VA has already committed time and resources to educate our workforce about the importance of data security.

Through formal training, printed communications, and other media, the focus is on good stewardship of data privacy. Our employees are now more aware about data management and security in the *administration … and in the delivery of services* to veterans and their families.

Our culture is changing. Change always takes great effort. It is disorienting and it is disruptive. But formerly acceptable business practices, as we have come to realize, are *simply no longer acceptable*. We are communicating this cultural reorientation across our Department, at all locations and at all levels. No one person, office, or Administration is exempt.

On February 21st, the Secretary convened an offsite meeting attended by all VA's senior leadership. He reviewed the recently issued information security directives and procedures as well as the information protection incidents and vulnerabilities. The Secretary reiterated, in no uncertain terms, his order that all supervisors fully execute their responsibilities in the area of information protection. In late March there will be a data security '*Update*' seminar for our senior leaders. In April, VA's annual Information Security Conference will address the theme of "*Strengthening* [IT] *Capabilities to Achieve the Gold Standard*." And in June, we will conduct Awareness Week and the systemic Security and Privacy Training ongoing across the Department.

We are working hard to achieve our goal—full protection of VA's sensitive data and information. We have made substantial progress in a relatively short timeframe … and we expect nothing less than continuous improvement. We have implemented corrective policies and procedures. Deployed the necessary technologies. Trained our workforce. And we will not relent in our efforts to ensure that every veteran's personal data is safe and secure.

While we have made great progress, we have clearly not fully achieved our objective. In our defense, I want to say that when data was lost, we did not stand still. We notified affected veterans by letter. We began investigations to determine root causes. We took preventive measures to improve security. And we communicated these incidents to the Congress. I don't believe there is any other Federal Department as forthcoming and public about this issue.

I can assure you we will continue work to improve our processes. We know all too well that lapses in information security … such as the one that occurred last year, and recently in Birmingham, weaken the confidence of our veterans, their families, and the American public in our ability to perform the mission that has been entrusted to us.

Mr. Chairman, that concludes my testimony. I will answer any questions that the Committee may have.

Prepared Statement of Hon. Robert T. Howard,
Assistant Secretary for Information and Technology,
U.S. Department of Veterans Affairs

Thank you, Mr. Chairman. I would like to expand on Deputy Secretary Mansfield's comments regarding the changes underway in the area of Information Technology. There are two specific areas I will focus on. First is the extensive reorganization taking place and second is the overarching program we have established to provide focus to all our remediation efforts.

The IT Realignment Program to transition the VA's IT Management System remains on track and is scheduled to be fully implemented by July 2008.

By April 1, 2007, software development employees and programs will be permanently reassigned to the CIO. This action follows the consolidation of operations and maintenance under the CIO, which was finalized beginning this FY. We are implementing a process based organizational structure, rooted in best practice processes that are aimed at correcting IT deficiencies that resulted in a loss of standardization, compatibility, interoperability and fiscal discipline. There are a total of four processes that are being introduced with the assistance of IBM, from a "best practices" standpoint. We have also developed a different organizational framework to provide focus in key areas. The Office of Information and Technology is now comprised of five major organizational elements, built around these core process areas. These will report to the CIO.

Each of the five major organizational elements is led by a Deputy CIO. One Deputy CIO is charged with directing the information protection and privacy protection programs in VA. This official is also responsible for risk assessment, risk mitigation, evaluation and assessment as it relates to information protection. The DCIO for Information Protection and Risk Management has already drafted regulations as required by the Veterans Benefits, Healthcare and Information Technology Act of 2006. The regulations will address at minimum, notification, data mining, fraud alerts, data breach analysis, credit monitoring, identity theft insurance and credit protection services.

To reach the "Gold Standard," as directed by the Secretary, we have implemented a new program to assess our information protection controls, develop plans to strengthen the controls where necessary, enforce the controls, and continuously monitor the information protection program. The action plan we have developed includes Development and Issuance of Policies and Procedures, Training and Education, Securing of Devices, Encryption of Data, Enhanced Data Security for VA's Sensitive Information, Enhanced Protection for Shared Data in Interconnected Systems, and Incident Management and Monitoring. A number of the specific requirements of the new law have already been introduced into our comprehensive plan. Regarding this plan I personally review progress on a weekly basis.

In closing, I believe we have made progress in improving IT operations in VA and we are working hard in partnership with the administrations and staff offices to improve our business practices to ensure the protection of veterans' sensitive information. Mr. Chairman, that concludes my testimony. I would be pleased to answer any questions that the Committee may have.

Prepared Statement of James P. Bagian, M.D., P.E.,
Chief Patient Safety Officer, Director, National Center for Patient Safety,
Veterans Health Administration, U.S. Department of Veterans Affairs

Mr. Chairman and Members of the Committee, I am pleased to be here today to discuss the issues of IT security, patient safety, culture and their relationships.

At the National Center for Patient Safety our mission is to prevent our patients being unintentionally harmed while under our care. This mission is quite large in scope and while most of our activities are concerned with direct clinical care they also address things that are a bit more removed such as safety during transport in vans, automatic doors and their potential to cause injury, and parking lot barrier design to name but a few. Similarly, the information system (IT) is also of great interest to us as our electronic health record (CPRS) is the tool that in large part is responsible for our ability to deliver the safe and high-quality care for which the VA has received many kudos and is a model for the country and world. While IT security is not intimately related to the direct clinical/physical safety of the patient we still view it as a relevant endeavor under the overall umbrella of preventing unintended harm to our patients, because issues such as identity theft can result in harm to our patients. In addition to direct harm, such as that which might be caused by someone successfully pretending to be a veteran getting care at VA facili-

ties, a larger and more wide-ranging harm can come from the energies expended responding to IT security issues. This redirection of resources can detract from our ability to render the medical care that is our basic mission.

The efforts of the National Center for Patient Safety have been based on creating an environment where problems can be identified in a timely manner, prioritized as to the appropriate action required, and analyzed to elicit the real underlying root causes and contributing factors. These steps result in the formulation of well-founded actions to mitigate risks. We often express this as three simple questions to be determined: What happened? Why did it happen? and What should be done to prevent it from happening in the future? We also have championed and implemented a system that promotes the extensive consideration of close calls, which are events where no significant harm befalls the patient. Studying close calls provides an opportunity to learn that is different from the traditional approach where learning begins only after a patient has suffered harm. The culture of the Veterans Health Administration has changed from one that was reactive to one that acts proactively to prevent undesirable outcomes. This did not happen overnight or by fiat. It happened through identifying problems that those at all levels of the organization perceived as real and worth tackling, and then removing the barriers that stood in the way of adopting more effective and risk-based strategies and techniques to prevent harm to patients. Through the implementation of a program that embraced these concepts and actively and aggressively solicited collaboration from all levels of the organization, as well as from stakeholders external to the organization such as Congressional committees, Veterans Service Organizations, and our unions, we have been able to make significant progress.

There is general agreement that the VA IT security efforts to date have not achieved the level of success as quickly as desired. There is little doubt that the VA has committed much effort to enhance the security of its IT systems and that the Secretary and senior management are dedicated and serious in their efforts to improve things. The real question at hand is why problems are still occurring. There are a myriad of factors, but I would like to point out several factors that may be worthy of consideration based on my experience and perspective.

Let me first state that there are no magic bullets here but there are some practices that have been applied in the area of patient safety as well as other areas that merit consideration. The use of root cause analysis (RCA) as developed by the VA National Center for Patient Safety (NCPS) has been a valuable tool that has identified the root causes and contributing factors behind many problems. These techniques include methodologies that go beyond the typical but ineffective initial questions such as "whose fault is this" to the three more meaningful and productive questions that I mentioned earlier: (1) What happened? (2) Why did it happen? and (3) What do we do to prevent it in the future? In fact, several years ago NCPS suggested to Secretary Principi that we be allowed to lead a multidisciplinary RCA team in response to the Blaster Worm problem that the IT world experienced. Secretary Principi agreed and chartered this team, and the result was extremely successful. In fact, on the 21st of February 2007 in a meeting between Mr. Howard and some of his top managers, including Mr. Shyshka, who worked with us on the Blaster Worm response, Mr. Shyshka brought up the fact that the group should currently consider employing the use of the RCA process on a widespread basis. The rationale he gave for this suggestion was the sustained success in preventing the reoccurrence of problems like that previously caused by the Blaster Worm. We agree with this suggestion and believe that the adoption of the RCA process might result in actions that are more effective than what we have experienced to date with regard to IT security. One important aspect of the RCA process is that it focuses on preventing future problems through understanding and mitigating the true underlying systems-based causative factors.

Some have indicated that what is needed is a culture change. While this may be true, culture changes do not happen by fiat or written directives. They happen through the creation of a shared vision of a goal that is deemed worthy, identification of the barriers to success through discussion at all levels of the organization and removal of these barriers, creation of tools and provision of the appropriate resources to accomplish the goals, and constant and unfettered communication both up and down the chain of command that encourages the candid identification of problems and appropriate responses to those problems. At the meeting with Mr. Howard mentioned above, the issue of communication and collaboration before the implementation of directives was discussed in an effort by all parties to maximize the chances of success. If this leads to a more proactive, collaborative, systems-based process that balances the security risks versus the clinical risks I think that meaningful progress can be made.

A suggestion would be to do a cultural/attitudinal survey of top and middle management that includes some frontline staff. A reason to survey senior leaders is that it is difficult to proceed, in this case toward improving culture and attitudes about IT security, if you don't know where you are starting from and why you are there.

In order to enhance the likelihood of success I believe that this Committee together with senior VA leadership needs to clearly communicate the types of approaches to be adopted. VA management and staff need to understand the various ramifications of the actions to be implemented, including schedules to be met and the expectations as to tradeoffs to be made to reduce risk. This kind of understanding was pivotal to the planning and implementation of the Patient Safety Program at the VA and without it the Patient Safety Program would have failed. There should be public acknowledgement that some IT security risk will always exist and that perfection is not possible. If such changes do not occur I am concerned that the security issues will not be resolved, and that clinical care will also suffer. This would result in our veterans losing in two ways.

Prepared Statement of Maureen Regan,
Counselor to the Inspector General,
Office of the Inspector General, U.S. Department of Veterans Affairs

INTRODUCTION

Mr. Chairman and Members of the Subcommittee, I am pleased to be here today to address the Office of Inspector General's (OIG's) oversight efforts of the Department of Veterans Affairs (VA) Information Security Program, its effectiveness, and the need for cultural change in VA to further improve and strengthen information security. Today, I will present our observations and identify the information security challenges VA must continue to address in order to ensure information security in VA. With me today is the Deputy Assistant Inspector General for Auditing, who will help answer questions about our audit work related to information security.

To improve the Department's information security posture, VA's senior management needs to effectively secure the Department's information assets. This includes the entire set of information technology (IT) systems and technological infrastructure, as well as all sensitive information and data under VA's control. It is critical that effective controls and monitoring mechanisms be in place to ensure compliance with applicable Federal standards and all VA policy requirements. Protecting VA information and data is, and must remain, a primary focus of the Department. Our observations indicate that VA needs a culture change throughout the Department to gain reasonable assurance of VA-wide compliance with Federal and Department information security regulations, policies, procedures, and guidance.

OIG HAS REPORTED CONTINUING WEAKNESSES IN INFORMATION SECURITY

Our audits and evaluations on information security and IT systems have shown the need for continued improvements in addressing security weaknesses and support the need to change VA's culture. We reported VA information security controls as a material weakness in our annual Consolidated Financial Statements (CFS) audits since the fiscal year (FY) 1997 audit. Our annual Federal Information Security Management Act (FISMA) audits have identified continuing information security vulnerabilities every year since FY 2001. We have also reported IT security as a major management challenge for the Department from FY 2000 to the present. As a result of these vulnerabilities, we recommended that VA pursue a more centralized approach, apply appropriate resources, and establish a clear chain of command and accountability structure to implement and enforce internal controls.

During the period 2000–2005, we reported that persistent repeat findings and weaknesses existed for physical, personnel, and electronic security and concluded that VA had not taken sufficient actions to correct the information weaknesses in our previous FISMA reports. Also, our work has continued to identify that corrective actions are not implemented at all VA facilities.

We observed that management of data centers and several program offices have taken actions to remediate elements of information security control weaknesses reported in our prior reports. However, VA's program and financial data continue to be at risk due to significant weaknesses related to the lack of effective implementation and enforcement of agencywide security controls. These weaknesses place sensitive information, including financial data and veterans' medical and benefit information, at risk of unauthorized access, improper disclosure, alteration, theft, or destruction, possibly occurring without detection.

Prior to the May 2006 data loss, VA's information security program showed significant security vulnerabilities. VA's CIO reported he did not have sole authority to implement all aspects of the VA-wide IT security program within VA's Administrations. IT infrastructure was decentralized because VA believed that decentralized operations provided better management of VA facilities. Finally, VA lacked adequate agencywide security control policies and procedures to provide effective guidance and organization standards.

VA has not fully implemented any of the recommendations on information security from our previous FISMA reports. In our ongoing 2006 FISMA audit, we determined that all 17 recommendations cited in prior FISMA reports remained unimplemented. In addition, we anticipate identifying several new high-risk areas associated with certification and accreditation of VA systems, remote access, and access to sensitive information by non-VA employees. Until all matters are fully addressed by the Department, VA systems and VA data remain at risk.

In some areas, however, the Department has made progress. Since the May 2006 data breach, VA has initiated positive steps focused on policies, awareness, and training. For example, all VA employees were mandated to complete information security awareness training. In addition, in 2006, VA took initial steps toward implementing a more centralized Departmentwide IT security program under the direction of the Department's CIO. However, establishing and implementing an effective centralized Departmentwide IT security program will require more time and effort.

VA DOES NOT ADEQUATELY PROTECT SENSITIVE INFORMATION FROM DISCLOSURE

The May 2006 theft of an employee's personal hard drive containing personal information on at least 26.8 million veterans, active military, and dependents, has been characterized as the largest data breach ever in the government. The employee, who was authorized access to the data, copied large amounts of protected information onto portable devices and took it home without authorization. The data was not encrypted or password-protected.

The incident was a wake-up call for VA because it identified the lack of effective policy and internal controls to protect sensitive information from theft, loss, or misuse by VA and contract employees. Our review found a patchwork of policies that were difficult to locate and fragmented. None of the policies prohibited the removal of protected information from the worksite or storing protected information on a personally owned computer, and did not provide safeguards for electronic data stored on portable media, such as laptop computers.

The potential loss of protected information not stored on a VA automated system highlighted a gap between VA policies implementing information laws and those implementing information security laws. We found that policies implementing information laws focused on identifying what information is to be protected and the conditions for disclosure; whereas, policies implementing information security laws focused on protecting VA automated systems from unauthorized intrusions and viruses. As a result, VA did not have policies in place at the time of the incident to safeguard protected information not stored on a VA automated system.

We found that policies implemented by the Secretary since the incident were a positive step in the right direction; however, we determined that more needed to be done to ensure protected information is adequately safeguarded. We determined that VA needed to enhance its policies for identifying and reporting incidents involving information violations and information security violations to ensure that incidents are promptly and thoroughly investigated; the magnitude of the potential loss is properly evaluated; and that VA management, appropriate law enforcement entities, and individuals and entities potentially affected by the incident are notified in a timely manner.

To address these deficiencies, we recommended that the Secretary take the following actions in our report, *Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans* (Report Number 06–02238–63, July 11, 2006).

- Establish one clear, concise VA policy on safeguarding protected information when stored or not stored in VA automated systems, ensure that the policy is readily accessible to employees, and that employees are held accountable for non-compliance.
- Modify the mandatory Cyber Security and Privacy Awareness training to identify and provide a link to all applicable laws and VA policy.
- Ensure that all position descriptions are evaluated and have proper sensitivity level designations, that there is consistency nationwide for positions that are similar in nature or have similar access to VA protected information and auto-

mated systems, and that all required background checks are completed in a timely manner.

- Establish VA-wide policy for contracts for services that requires access to protected information and/or VA automated systems, that ensures contractor personnel are held to the same standards as VA employees, and that information accessed, stored, or processed on non-VA automated systems is safeguarded.
- Establish VA policy and procedures that provide clear, consistent criteria for reporting, investigating, and tracking incidents of loss, theft, or potential disclosure of protected information or unauthorized access to automated systems, including specific timeframes and responsibilities for reporting within the VA chain-of-command and, where appropriate, to OIG and other law enforcement entities, as well as appropriate notification to individuals whose protected information may be compromised.

The Secretary concurred with the findings and recommendations in our report and agreed to implement the recommendations. On February 9, 2007, the Assistant Secretary for Information and Technology and his staff provided us with a briefing on the status of the recommendations in the report. Although an implementation process was discussed using an electronic database with a matrix that showed what issues needed to be addressed, we were not provided an implementation plan or any supporting documentation, such as draft policies, to show progress made in implementing the recommendations. To date, all 5 recommendations remain open, although VA has developed a new Privacy Awareness training module. It was circulated to all VA Privacy Officers, including the OIG's Privacy Officer, for review and comment. We reviewed the module and confirmed that it provides a link to applicable laws and VA policy. When implemented, the module will meet the intent of one of our recommendations.

Shortly after the May 2006 incident, VA issued policies to address information security. On June 7, 2006, the Secretary issued VA Directive 6504, *Restrictions on Transmission, Transportation and Use of, and Access to, VA Data Outside VA Facilities*, and it is available to all employees on VA's directives Web site. VA Directive 6504 contains policy for 23 different items. As stated in our report, we found that the Directive was difficult to understand; too technical for the average employee to understand; used terms, such as "appropriate" that were too vague to ensure compliance; and made reference to other applicable policies, guidelines, and laws without identifying them.

Notwithstanding these concerns, we considered VA Directive 6504 to be a step in the right direction. The Directive prohibits the use of non-VA owned equipment to access the VA Intranet remotely or to process VA protected information except as provided in the Directive. In addition to requiring the use of encryption software on computers used outside VA facilities, a key provision in the Directive is that only VA-owned equipment, including laptops and handheld computers, may be used when accessing VA systems remotely. However, these requirements have not been implemented throughout VA. On October 5, 2006, VA issued a Memorandum, IT Directive 06–5, approving a temporary waiver for all three VA Administrations. Although the VA personnel were required to use approved encryption software when using non-VA hardware, VA does not provide the software. In addition, neither VA Directive 6504 nor IT Directive 06–5 contain provisions stating how VA will ensure compliance.

There is a greater awareness in VA regarding the issue. However, VA still lacks effective internal controls and accountability which leaves sensitive information at risk.

VA CONTINUES TO REPORT ONGOING DATA INCIDENTS

VA's Security Operations Center (SOC) is responsible for managing, protecting, and monitoring the cyber security posture of the agency. In July 2006, VA began sending us information on incidents from the SOC, providing information on a variety of incidents such as unauthorized access; missing, stolen, or lost laptop computers; improper disposal; and numerous incidents involving unencrypted e-mail messages containing sensitive information.

To date, these reports have covered about 3,600 incidents and the SOC has referred over 250 incidents to us, which resulted in us opening 46 cases to investigate. SOC reports do not always include indications of the magnitude of the data breach, that is, the number of individuals with personally identifiable information related to the incident. We have no way to determine the number and magnitude of incidents that occurred and were not reported to the SOC, nor can we verify the accuracy on the reported number of individuals affected by data incidents listed in SOC reports.

Since the May 2006 incident, the OIG has remained committed to investigating significant data loss cases that show that VA or contract employees are not taking the steps necessary to protect sensitive information. For example, the incident involving the theft of a computer owned and maintained by Unisys, containing sensitive VA information, shows that information provided to contractors is also at risk. In our ongoing investigation of the data loss at Birmingham, Alabama, we continue to find that VA sensitive information was not protected.

CONTINUING CHALLENGES

Information security weaknesses persist at VA despite the findings and recommendations made in our reports. Most VA data remains unencrypted, including data transmitted by electronic mail over the Internet. Although the Department has begun action, it still does not know how many VA employees and contractors use non-VA computers to remotely access VA systems. In addition, VA has not determined how many external hard drives or other portable devices are in use throughout VA. Finally, VA does not know what VA data is stored on these computers, external hard drives, or other portable devices. VA also has no means to monitor whether access to data by employees and contractors is limited to the information needed to conduct business.

Policies and procedures issued to safeguard protected information will not be effective unless there is compliance by all employees and contract personnel who have access to the information. Local management needs to conduct adequate oversight to ensure compliance and hold employees and contractors accountable for noncompliance. VA must ensure that managers and supervisors are held accountable for implementing the policies and procedures. In addition, VA must invest in the resources needed to provide employees with the hardware and software needed to conduct business and, at the same time, protect sensitive information.

Implementing the controls needed to ensure that sensitive information is protected will require that VA employees change the manner in which they currently conduct business. VA must find a way to implement these controls without impacting VA's ability to meet its mission.

In closing, I would like the Subcommittee to know that oversight and reviews of the effectiveness of VA's information security will remain a priority for the OIG until these issues are addressed. We remain committed to assessing the adequacy of information security controls and we will remain dedicated to protecting our Nation's veterans along with their personal and sensitive information. Mr. Chairman and Members of the Subcommittee, thank you again for this opportunity to update you on the status of our ongoing work. We are happy to answer any questions.

Prepared Statement of Gregory C. Wilshusen, Director, Information Security Issues, U.S. Government Accountability Office

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on information security management at the Department of Veterans Affairs (VA). For many years, GAO has identified information security as a governmentwide high-risk issue [1] and emphasized its criticality for protecting the government's information assets. GAO has issued over 15 reports and testimonies and made over 150 recommendations from 1998 to 2005 related to VA's information security program.

Today I will address VA's information security management, including weaknesses that GAO and others have reported, as well as actions that the Department has taken to resolve these deficiencies. I will also discuss ongoing audit work that GAO is conducting at VA.

To describe VA's information security management, we reviewed our previous work in this area, as well as reports by the Department and its Office of Inspector General (IG). To provide additional context, we have included, as an attachment, a list of key GAO publications related to VA security issues. All GAO work conducted for this testimony is in accordance with generally accepted government auditing standards.

Results in Brief

Significant concerns have been raised over the years about VA's information security—particularly its lack of a robust information security program, which is vital

[1] GAO, *High-Risk Series: An Update*, GAO–07–310 (Washington, D.C.: January 2007); *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*, GAO–05–552 (Washington, D.C.: July 15, 2005).

to avoiding the compromise of government information. We have previously reported on wide-ranging deficiencies in VA's information security controls.[2] For example, VA had not consistently implemented appropriate controls for (1) limiting, preventing, and detecting electronic access to sensitive computerized information; (2) restricting physical access to computer and network equipment to authorized individuals; (3) segregating incompatible duties among separate groups or individuals; (4) ensuring changes to computer software were authorized and timely; and (5) providing continuity of computerized systems and operations. The Department's IG has recently identified similar weaknesses. These longstanding deficiencies existed, in part, because VA had not implemented key components of a comprehensive, integrated information security program. Although the Department has taken steps to implement components of its security program, its efforts have not been sufficient to effectively protect its information and information systems. As a result, sensitive information remains vulnerable to inadvertent or deliberate misuse, loss, or improper disclosure.

We have several ongoing engagements to perform work at VA to review the Department's efforts in improving its information security and information technology management. Our ongoing work is examining data breach notification, actions to strengthen information security controls, controls over information technology equipment, and implementation of an information technology realignment initiative.

Background

Information security is a critical consideration for any organization that depends on information systems and networks to carry out its mission or business. The security of these systems and data is essential to prevent data tampering, disruptions in critical operations, fraud, and the inappropriate disclosure of sensitive information. Recognizing the importance of securing Federal systems and data, Congress passed the Federal Information Security Management Act (FISMA) in 2002, which set forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.[3]

Under FISMA, agencies are required to provide sufficient safeguards to cost-effectively protect their information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, including controls necessary to preserve authorized restrictions on access and disclosure. The Act requires each agency to develop, document, and implement an agencywide information security program that is to include assessing risk; developing and implementing policies, procedures, and security plans; providing security awareness and training; testing and evaluating the effectiveness of controls; planning, implementing, evaluating, and documenting remedial action to address information security deficiencies; detecting, reporting, and responding to security incidents; and ensuring continuity of operations.

In providing health care and other benefits to veterans and their dependents, VA relies on a vast array of computer systems and telecommunications networks to support its operations and store sensitive information, including personal information on veterans. Effectively securing these computer systems and networks is critical to the Department's ability to safeguard its assets and sensitive information.

VA's Information Security Weaknesses Are Long Standing

VA has faced longstanding challenges in achieving effective information security across the Department. Our previous reports and testimonies[4] have identified wide-ranging, often recurring deficiencies in the Department's information security controls. For example, VA had not consistently implemented appropriate controls for (1) limiting, preventing, and detecting electronic access to sensitive computerized information; (2) restricting physical access to computer and network equipment to authorized individuals; (3) segregating incompatible duties among separate groups or individuals; (4) ensuring changes to computer software were authorized and timely; and (5) providing continuity of computerized systems and operations. Figure 1 details the information security control weaknesses we identified at VA from 1998 through 2005.

---

[2] See attachment 1.

[3] FISMA, Title III, E–Government Act of 2002, Pub. L. 107–347 (Dec. 17, 2002).

[4] Attachment 1 includes a list of our products related to information technology vulnerabilities at VA.

Figure 1: Chronology of Information Security Weaknesses Identified by GAO

Year	GAO report	VA location or agency	Information security control areas: Access control	Physical security	Segregation of duties	Change control	Service continuity	Security program
1998	GAO/AIMD-98-175	Austin	●	●	●	●	●	●
		Dallas	●	●			●	●
		Albuquerque	●	●	●		●	●
		Hines	●	■	■	■	■	●
		Philadelphia	●	■	■	■	■	●
1999	GAO/AIMD-99-161	Austin	●			●		●
2000	GAO/AIMD-00-232	Maryland	●	●	●	●	●	●
		New Mexico	●	●	●	●	●	●
		North Texas/Dallas	●	●	●		●	●
2000	GAO/AIMD-00-5	VA	●		●			●
2002	GAO-02-703	VA	■	■	■	■	■	●
2005	GAO-05-552	VA	●	■	●	●	●	●

● Weakness found in this area

■ Control area not included in scope of audit

Source: GAO reports.

Notes: Hines is a suburb of Chicago.
Full citations are provided in attachment 1.

These weaknesses existed, in part, because VA had not implemented key components of a comprehensive information security program. Specifically, VA's information security efforts lacked:

- Clearly delineated security roles and responsibilities;
- Regular, periodic assessments of risk;
- Security policies and procedures that addressed all aspects of VA's interconnected environment;
- An ongoing security monitoring program to identify and investigate unauthorized, unusual, or suspicious access activity; and
- A process to measure, test, and report on the continued effectiveness of computer system, network, and process controls.

We made a number of recommendations in 2002 that were aimed at improving VA's security management.[5] Among the primary elements of these recommendations were that VA centralize its security management functions and perform other actions to establish an information security program, including actions related to risk assessments, security policies and procedures, security awareness, and monitoring and evaluating computer controls.[6]

Since our report in 2002, VA's independent auditors and its IG have continued to report serious weaknesses with the Department's information security controls. In the auditors' report on internal controls prepared at the completion of VA's 2006 financial statement audit, information technology security controls were identified as a material weakness because of serious weaknesses related to access control, segregation of duties, change control, and service continuity.[7] These areas of weakness are virtually identical to those that we had identified years earlier.

The Department's *FY 2006 Annual Performance and Accountability Report* states that the IG continues to identify the same vulnerabilities and make the same recommendations year after year. The IG's September 2006 audit of VA's information security program noted that 16 previously reported recommendations remained unimplemented; it also identified a new weakness and made an additional rec-

[5] GAO, *Veterans Affairs: Sustained Management Attention Is Key to Achieving Information Technology Results*, GAO–02–703 (Washington, D.C.: June 12, 2002).

[6] We based our recommendations on guidance and practices provided in GAO, *Federal Information System Controls Audit Manual*, GAO/AIMD–12.19.6 (Washington, D.C.: January 1999); *Information Security Management: Learning from Leading Organizations*, GAO/AIMD–98–68 (Washington, D.C.: May 1998); *Information Security Risk Assessment: Practices of Leading Organizations*, GAO/AIMD–00–33 (Washington, D.C.: November 1999); and Chief Information Officer Council, *Federal Information Technology Security Assessment Framework* (Washington, D.C.: Nov. 28, 2000). The provisions of FISMA (passed in late 2002) and associated guidance were generally consistent with this earlier guidance.

[7] The auditor's report is included in VA's *FY 2006 Annual Performance and Accountability Report*.

ommendation. The IG has reported information technology security as a major management challenge for the Department each year for the past 6 years.

VA's Efforts to Address Information Security Weaknesses Have Been Limited

Despite having taken steps to address the weaknesses described in our earlier work, VA has not yet resolved these weaknesses on a Departmentwide basis or implemented a comprehensive information security program.[8] For example:

- *Central security management function:* In October 2006, the Department moved to a centralized management model. The Department has also contracted for project support in helping to frame a security governance structure and provide tools to assist management with controls over information technology assets. This work is scheduled to be completed in March 2007.
- *Periodic risk assessments:* VA is implementing a commercial tool to identify the level of risk associated with system changes and also to conduct information security risk assessments. It also created a methodology that establishes minimum requirements for such risk assessments. However, it has not yet completed its risk assessment policy and guidance. While the policy and guidance were originally scheduled to be completed by the end of 2006, the completion date was extended to April 2007.
- *Security policies and procedures:* VA is in the process of developing policies and directives to strengthen security controls as part of its action plan. For example, VA planned to develop directives by the end of 2006 on access controls and media protection, standards for restricting use of portable and mobile devices, and policies regarding physical access to VA computer rooms. However, the completion date for development of these policies has been extended to April 2007.
- *Security awareness:* VA has taken steps to improve security awareness training. It holds an annual Department information security conference, and it has developed a Web portal for security training, policy, and procedures, as well as a security awareness course that VA employees are required to review annually. However, VA has not demonstrated that it has a process to ensure compliance.
- *Monitoring and evaluating computer controls:* VA has taken steps to improve the monitoring and evaluating of computer controls by developing policies and procedures. For example, VA planned to develop by the end of 2006 criteria for system security control testing at least every 3 years and planned to identify key system security controls for testing on a routine basis. However, the completion dates for development of these policies have been extended to April 2007.

To fulfill our recommendations in these areas, VA must not only complete and document the policies, procedures, and plans that it is currently developing, but also implement them effectively. With regard to its IG's findings and recommendations, the Department has established an action plan to address the material weakness in information security (Data Security—Assessment and Strengthening of Controls), which is to correct deficiencies and eliminate vulnerabilities in this area. Despite these actions, the Department has not implemented the key elements of a comprehensive security management program, and its efforts have not been sufficient to effectively protect its information systems and information, including personal information, from unauthorized disclosure, misuse, or loss.

GAO Has Ongoing Reviews of Information Technology and Security Issues at VA

We have several ongoing engagements to perform work at VA to review the Department's efforts in improving its information security and information technology management. These engagements address:

- *Data breach notification:* We are conducting a study to determine the lessons that can be learned from the VA data breach with respect to notifying government officials and affected individuals about data breaches. For this evaluation, we are examining similar data breach cases at other Federal agencies, as well as analyzing Federal guidance on data breach notification procedures.
- *Actions to strengthen information security controls:* We are conducting a review to evaluate VA's efforts to implement prior GAO and IG information security-related recommendations and to assess actions VA has taken since the data

[8] This result is also reflected in the Department's failing grade in the annual report card on computer security that was issued by the then House Committee on Government Reform: *Computer Security Report Card* (Washington, D.C.: Mar. 16, 2006).

breach of May 3, 2006, to strengthen information security and protect personal information. As part of this engagement, we are examining VA's timeline of planned efforts to strengthen controls.

- *Controls over information technology equipment:* We are conducting a followup audit[9] at selected VA locations to determine the risk of theft, loss, or misappropriation of information technology equipment. To perform our audit, we are assessing the effectiveness of physical inventory controls and the property disposal process at four VA locations.
- *VA's information technology realignment initiative:* We are conducting a review to determine whether VA's realignment plan for its Office of Information and Technology includes critical factors for successful implementation of a centralized management model. We are also looking at how the realignment will ensure that under the centralized management approach, the chief information officer is accountable for the entire information technology budget (including those funds that had been administered by the Veterans Health Administration and Veterans Benefits Administration). In performing this evaluation, we are analyzing governance and implementation plans, as well as budgetary and other relevant documentation.

In summary, longstanding information security control weaknesses at VA have placed its information systems and information at increased risk of misuse and unauthorized disclosure. Although VA has taken steps to mitigate previously reported weaknesses, the Department has not yet resolved these weaknesses, implemented the recommendations of GAO and the IG, or implemented a comprehensive information security program, which it needs in order to effectively manage risks on an ongoing basis. Much work remains to be done. Only through strong leadership, sustained management commitment and effort, disciplined processes, and consistent oversight can VA address its persistent, longstanding control weaknesses.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions you or other Members of the Subcommittee may have.

Contact and Acknowledgments

If you have any questions concerning this statement, please contact Gregory C. Wilshusen, Director, Information Security Issues, at (202) 512–6244, wilshuseng@gao.gov. Other individuals who made key contributions include Barbara Collier, Mary Hatcher, Valerie Hopkins, Leena Mathew, and Charles Vrabel.

Attachment 1: Selected GAO Products

Information Security: Leadership Needed to Address Weaknesses and Privacy at Veterans Affairs. GAO–06–897T. Washington, D.C.: June 20, 2006.

Veterans Affairs: Leadership Needed to Address Security Weaknesses and Privacy Issues. GAO–06–866T. Washington, D.C.: June 14, 2006.

Privacy: Preventing and Responding to Improper Disclosures of Personal Information. GAO–06–833T. Washington, D.C.: June 8, 2006.

Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements. GAO–05–552. Washington, D.C.: July 15, 2005.

Veterans Affairs: Sustained Management Attention is Key to Achieving Information Technology Results. GAO–02–703. Washington, D.C.: June 12, 2002.

Major Management Challenges and Program Risks: Department of Veterans Affairs. GAO–01–255. Washington, D.C.: January 2001.

VA Information Systems: Computer Security Weaknesses Persist at the Veterans Health Administration. GAO/AIMD–00–232. Washington, D.C.: September 8, 2000.

Information Systems: The Status of Computer Security at the Department of Veterans Affairs. GAO/AIMD–00–5. Washington, D.C.: October 4, 1999.

VA Information Systems: The Austin Automation Center Has Made Progress in Improving Information System Controls. GAO/AIMD–99–161. Washington, D.C.: June 8, 1999.

Information Systems: VA Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure. GAO/AIMD–98–175. Washington, D.C.: September 23, 1998.

[9] This is a followup audit to work reported in GAO, *VA Medical Centers: Internal Control Over Selected Operating Functions Needs Improvement*, GAO–04–755 (Washington, D.C.: July 21, 2004).

GAO Highlights

Information Security: Veterans Affairs Needs to Address Long-Standing Weaknesses

Why GAO Did This Study

Security breaches at the Department of Veterans Affairs (VA) and other public and private organizations have highlighted the importance of well-designed and implemented information security programs. GAO was asked to testify on its past work on VA's information security program, as well as ongoing reviews that it is conducting at VA.

In developing its testimony, GAO drew on over 15 of its previous reports and testimonies, as well as reports by the Department's Inspector General (IG).

What GAO Recommends

To ensure that security issues are adequately addressed, GAO has previously made over 150 recommendations to VA on implementing effective controls and developing a robust information security program.

What GAO Found

For many years, GAO has raised significant concerns about VA's information security—particularly its lack of a comprehensive information security program, which is vital to safeguarding government information. The figure below details information security weaknesses that GAO identified from 1998 to 2005. As shown, VA had not consistently implemented appropriate controls for (1) limiting, preventing, and detecting electronic access to sensitive computerized information; (2) restricting physical access to computer and network equipment to authorized individuals; (3) segregating incompatible duties among separate groups or individuals; (4) ensuring that changes to computer software were authorized and timely; or (5) providing continuity of computerized systems and operations. The Department's IG has also reported recurring weaknesses throughout VA in such areas as access controls, physical security, and segregation of incompatible duties. In response, the Department has taken actions to address these weaknesses, but these have not been sufficient to establish a comprehensive information security program. As a result, sensitive information has remained vulnerable to inadvertent or deliberate misuse, loss, or improper disclosure. Without an established and implemented security program, the Department will continue to have major challenges in protecting its systems and information from security breaches.

GAO has several ongoing engagements to review the Department's efforts in improving its information security and information technology management. These engagements address:

- Data breach notification;
- Actions to strengthen information security controls;
- Controls over information technology equipment; and
- VA's information technology realignment effort.

SUBMISSION FOR THE RECORD

Prepared Statement of Hon. Zackary T. Space, a Representative in Congress from the State of Ohio

Dear Members of the Subcommittee and Panelists,

I would like to submit for the record my most sincere apologies for my absence this afternoon. An unexpected family emergency has called me away from my congressional duties. While I would like very much to be in attendance today to review the important information and security management procedures in place at the VA, I must be with my mother on the loss of her husband.

I appreciate your understanding on this matter. Please know that I remain committed as ever to the important work of this Subcommittee and those that it serves.

Sincerely,

ZACK SPACE.